



UNITED STATES MARINE CORPS
MARINE CORPS BASE
QUANTICO, VIRGINIA 22134-5001

MCBO P5510.1B
B 054
3 Dec 01

MARINE CORPS BASE ORDER P5510.1B w/Ch 1

From: Commanding General, Marine Corps Base, Quantico, VA
(B 054)

To: Distribution List

Subj: DEPARTMENT OF NAVY INFORMATION AND PERSONNEL SECURITY
PROGRAM

Ref: (a) SECNAVINST 5510.30A
(b) SECNAVINST 5510.36
(c) OPNAVINSNT C5510.93E (NOTAL)
(d) MCO P5510.18A
(e) JAGINST 5800.7C
(f) DoD 5220.22-M
(g) OPNAVINST 5513.1E (NOTAL)
(h) OPNAVINST 5513.10B (NOTAL)
(i) SECNAVINST 5720.44A
(j) SECNAVINST 5212.5D
(k) NCPCINST 5521.1 (NOTAL)
(l) MCO P1070.12K
(m) MCO P1080.40B
(n) DoD 5210.2 (NOTAL)
(o) OPNAVINST C5510.101 (NOTAL)
(p) OPNAVINST S5511.35 (NOTAL)
(q) SECNAVINST 5212.5D
(r) MCBO 5210.2A
(s) MCBO 5230.3
(t) MCO 5510.17

Encl: (1) Locator Sheet

1. Purpose. To provide Marine Corps Base (MCB), Marine Corps Combat Development Command (MCCDC) and tenants covered by Inter Service Support Agreements (ISA) with the regulations and guidelines for managing classified information and personnel security per the references.

2. Cancellation. MCBO P5510.1A.

3 Dec 01

3. Objective. To ensure maximum uniformity and effectiveness in the application of the Information and Personnel Security Program aboard MCB, Quantico.

4. Summary of Revision. This manual contains modifications designed to clarify and provide a more comprehensive understanding of the Information and Personnel Security Program as it pertains to the mission of this Base and its activities.

5. Recommendations. Recommendations concerning the Information and Personnel Security Program are invited and may be submitted to the CG MCB (B 054) via the appropriate chain of command.

6. Certification. Reviewed and approved this date.

A handwritten signature in black ink, appearing to read 'D. L. Wright', is positioned above the printed name and title.

D. L. WRIGHT
Chief of Staff

DISTRIBUTION: INTERNET



UNITED STATES MARINE CORPS
MARINE CORPS BASE
QUANTICO, VIRGINIA 22134-5001

MCBO P5510.1B Ch 1
B 054
19 Nov 03

MARINE CORPS BASE ORDER P5510.1B Ch 1

From: Commander
To: Distribution List

Subj: DEPARTMENT OF NAVY INFORMATION AND PERSONNEL SECURITY
PROGRAM

Encl: (1) New page inserts to MCBO P5510.1B

1. Purpose. To transmit new page inserts to the basic Order.
2. Action. Remove pages iii, 19-1, 19-3, and 19-4 and replace with the corresponding pages contained in the enclosure.
3. Change Notation. Paragraphs denoted by an asterisk (*) symbol contain changes not previously published.
4. Filing Instructions. File this Change transmittal immediately following the signature page of the basic Order.

A handwritten signature in black ink, appearing to read "R. T. Bright", is positioned above the printed name and title.

R. T. BRIGHT
Chief of Staff

DISTRIBUTION: INTERNET

LOCATOR SHEET

Subj: DEPARTMENT OF THE NAVY INFORMATION AND PERSONNEL SECURITY
PROGRAM

Location: _____
(Indicate the location(s) of the copy(ies) of this Manual.)

INFORMATION AND PERSONNEL SECURITY PROGRAM

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Incorporated Change

INFORMATION AND PERSONNEL SECURITY PROGRAM

TABLE OF CONTENTS

CHAPTER

1	INTRODUCTION TO THE INFORMATION AND PERSONNEL SECURITY PROGRAM
2	COMMAND SECURITY MANAGEMENT
3	COUNTERINTELLIGENCE MATTERS AND NATIONAL SECURITY
4	SECURITY EDUCATION
5	PERSONNEL SECURITY INVESTIGATIONS
6	PERSONNEL SECURITY DETERMINATIONS
7	CLEARANCE
8	ACCESS to CLASSIFIED INFORMATION
9	CONTINUOUS EVALUATIONS
10	VISITOR ACCESS to CLASSIFIED INFORMATION
11	CLASSIFICATION MANAGEMENT
12	SECURITY CLASSIFICATION GUIDES
13	MARKING
14	SAFEGUARDING
15	DISSEMINATION
16	TRANSMISSION AND TRANSPORTATION
17	STORAGE AND DESTRUCTION
18	INDUSTRIAL SECURITY PROGRAM
* 19	LOSS, COMPROMISE, AND OTHER SECURITY VIOLATIONS

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 1

INTRODUCTION TO THE INFORMATION AND PERSONNEL SECURITY PROGRAM

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	1000	1-3
AUTHORITY	1001	1-3
APPLICABILITY	1002	1-3
RESPONSIBILITY FOR COMPLIANCE	1003	1-4
SPECIAL ACCESS PROGRAMS (SAP)	1004	1-4

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 1

INTRODUCTION TO THE INFORMATION AND PERSONNEL SECURITY PROGRAM

1000. BASIC POLICY. The Marine Corps Base (MCB) Information and Personnel Security Program is established in compliance with the Department of the Navy (DON) Program to ensure that information classified under the authority of Executive Order 12968 is protected from unauthorized disclosure and that appointment of civilian employees, acceptance or retention of military personnel in the Navy and Marine Corps and granting access to classified information or assignment to sensitive duties is clearly consistent with the interest of national security and in compliance with Executive Order 10450, Security Requirements for Government Employees, Department of Defense (DoD) 5200.2-R, DoD Personnel Security Program Regulations.

1001. AUTHORITY

1. The CG MCB is responsible for establishing and maintaining an Information and Personnel Security Program in compliance with reference (a) and (b).
2. The responsibility for the security and proper handling of classified material extends directly to the individual having knowledge or possession of such material and to activity heads within whose purview classified material is utilized.
3. Individual requests for guidance or interpretation of this manual should be addressed to the CG MCB (B 054). Attn: Command Security Manager.

1002. APPLICABILITY

1. This manual establishes coordinated policies for the security of classified information and for personnel security matters incorporating the policies of numerous DoD/DON Directives. It is not expected that these directives will or can ensure absolute security at this Base. Rather, they permit the accomplishment of essential tasks while affording selected items of information reasonable degrees of security with a minimum risk.

2. As this manual establishes coordinated policies for maintenance of the Information and Personnel Security Program it is applicable to all organizations and activities stationed aboard this Base. References (a), (b) and this manual will provide the basis for handling the Information and Personnel Security Program aboard this Base.

1003. RESPONSIBILITY FOR COMPLIANCE

1. Activity heads are responsible for compliance with and implementation of this manual within their activity.
2. Each individual, military or civilian, in or employed by the Navy or Marine Corps, is responsible for compliance with this manual in all respects.
3. All activities that hold, handle or otherwise come in contact with classified information will at a minimum have on hand and maintain references (a), (b) and this manual.

1004. SPECIAL ACCESS PROGRAMS (SAP). These programs will be handled per the guidelines contained in SECNAVINST 5510.30A, 5510.36 and other directives. The Base Special Security Officer (SSO) will act as coordinator for the SAPs and sensitive compartmented information in cooperation with the CG MCB (B 054).

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 2

COMMAND SECURITY MANAGEMENT

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	2000	2-3
BASE MANAGEMENT	2001	2-3
APPOINTMENT OF ORGANIZATIONAL SECURITY MANAGERS	2002	2-4
OTHER APPOINTMENTS	2003	2-5
SECURITY MANAGEMENT/SPECIAL SECURITY OFFICER COORDINATION	2004	2-6
INTER-SERVICE SUPPORT AGREEMENTS.	2005	2-6
COMMAND SECURITY PROCEDURES	2006	2-7
EMERGENCY PLANS	2007	2-7
INSPECTIONS AND REVIEW	2008	2-7
UNANNOUNCED SECURITY INSPECTIONS	2009	2-8
COUNTERINTELLIGENCE TECHNICAL ASSISTANCE	2010	2-9
FIGURE		
2-1	SAMPLE SECURITY MANAGER APPOINTMENT LETTER	2-10
2-2	SAMPLE DESIGNATION OF AUTHORIZED RECIPIENTS FOR CLASSIFIED MATERIAL LETTER.	2-11

INFORMATION AND PERSONNEL SECURITY PROGRAM

FIGURE

2-3	SAMPLE TOP SECRET CONTROL OFFICER APPOINTMENT LETTER.	2-12
2-4	SAMPLE SECONDARY CONTROL POINT CUSTODIAN APPOINTMENT LETTER.	2-13
2-5	SAMPLE INFORMATION SYSTEMS SECURITY OFFICER APPOINTMENT LETTER.	2-14
2-6	SAMPLE INFORMATION SYSTEMS SECURITY COORDINATOR APPOINTMENT LETTER.	2-15
2-7	SAMPLE ACTIVITY SECURITY CHECKLIST. . .	2-16
2-8	SAMPLE SECURITY CONTAINER CHECK SHEET	2-17

EXHIBIT 2A

INFORMATION AND PERSONNEL SECURITY PROGRAM INSPECTION CHECKLIST

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 2

COMMAND SECURITY MANAGEMENT

2000. BASIC POLICY

1. Terminology. "Command" is used as a generic term for any organizational entity and may include a base, station, unit, laboratory, installation, facility, center, activity, detachment, squadron, ship, etc. "Commanding Officer" is used throughout this regulation as a generic term for the head of any DON command and includes commander, commanding general, director, officer in charge, etc.
2. Commanding officers/directors/activity heads are responsible for compliance with and the implementation of the DON Information and Personnel Security Program within their organizations.

2001. BASE MANAGEMENT

1. The Information and Personnel Security Program establishes a network of personnel throughout this Base to supervise and ensure effective security, control, and utilization of classified material.
2. To ensure proper handling and control of classified material, the following appointments by the CG MCB will be made in writing, setting forth the requirements that they be familiar with the specific portions of SECNAVINST 5510.30A, SECNAVINST 5510.36 and other directives as may pertain:
 - a. Command Security Manager - Supervisory Security Specialist
 - b. Command Assistant Security Manager - Security Specialist
 - c. Top Secret Control Officer - Head, Classified Material Control Center (CMCC).
 - d. Primary Custodian Classified Material - Head, CMCC.
 - e. Responsible Officer, Communications Security Material System (CMS) - Head, CMCC.

f. Electronic Keying Material Systems (EKMS), Manager/Custodian - Security Specialist, CMCC.

g. Responsible Officer, STU-III COMSEC Keying Material Account - Head, CMCC.

h. Custodian, Naval Warfare Publications - Security Specialist, CMCC.

i. North Atlantic Treaty Organization/Critical Nuclear Weapons Design Information Control Officer - Head, CMCC.

j. Contracting Officer's Representative (COR) - Command Assistant Security Manager.

k. Information Systems Security Manager (ISSM) - Command Security Manager.

l. Special Security Officer (SSO) - Chief, Intelligence Division, Marine Corps Intelligence Activity (MCIA).

2002. APPOINTMENT OF ORGANIZATIONAL SECURITY MANAGERS

1. In addition to the MCB Command Security Manager, one security manager will be appointed in writing for each major activity. This appointment will be a 0-4/GS-11 or above who will be responsible for the Information and Personnel Security Program, which includes industrial security when appropriate. These managers will serve as direct representatives of the Command Security Manager. As such, they will keep the Command Security Manager informed of all security violations and/or related problems. Each newly appointed security manager will be enrolled in (and have completed within 6 months) the prescribed "Security Managers" training course offered by the Personnel Security Office (PSO), Security Branch.

2. An appointing letter will be prepared for individuals serving in security functions, with a copy forwarded to the Command Security Manager (B 054). Figure 2-1 is a sample appointment letter. Security managers will further comply with the duties and responsibilities as prescribed in Chapter 2 of SECNAVINST 5510.30A and SECNAVINST 5510.36.

3. All activities identify as Secondary Control Points (SCP) will also designate personnel who are authorized to receipt for classified material. Names listed as personnel authorized to receipt for classified material (figure 2-2) must also be listed on at least one of the unit(s) SF 700 envelope(s) (figure 13-1)

2003. OTHER APPOINTMENTS

1. Each activity that anticipates the possibility of handling or viewing Top Secret information will appoint a Top Secret Control Officer (TSCO) in writing. Individuals appointed must be an E-7/GS-07 or above and have a final Top Secret security clearance and access. Additional requirements and duties of the TSCO are set forth in Chapter 2 of SECNAVINST 5510.30A, which will be referenced in the letter of appointment, with a copy to the CG MCB (B 054). Figure 2-3 is a sample appointment letter.

2. Activity heads may, as needed, designate Top Secret Control Assistants. Personnel so designated must be an E-5/GS-05 or above and have been granted a final Top Secret security clearance and access. The requirements and duties of the assistant are contained in chapter 2 of SECNAVINST 5510.30A, which will be referenced in the letter of appointment, with a copy forwarded to the CG MCB (B 054). The designation of a Top Secret Control Assistant does not relieve the TSCO of any responsibility for the control and protection of Top Secret material.

3. Activity heads that hold classified material will appoint a classified material custodian in writing. Individuals so assigned are responsible for ensuring that the control, handling, and security procedures for classified material within their respective activities are conducted per the provisions of SECNAVINST 5510.36 and this manual. A custodian appointed by the activity must be an E-4/GS-05 or above and complete training by the Command Security Manager (B 054) prior to assuming the unit's classified holdings. Criteria, requirements, and duties will be referenced in the letter of appointment, with copies forwarded to the Command Security Manager (B 054). Figure 2-4 is a sample appointment letter.

4. Per reference (b), each activity involved in processing data in an automated information system (AIS) must designate, in writing, an Information Systems Security Officer (ISSO). The requirements and duties of the ISSO are contained in chapter 2 of SECNAVINST 5510.36. The ISSO will be responsible to the organizational security manager for

protection of information, regardless of the classification, being processed on the AIS. The ISSO will be responsible for implementing and maintaining information system and network security requirements. Additionally, each major sub-element of the activity will appoint an Information Systems Security Coordinator (ISSC) to assist the ISSO and act as the end-user point of contact. Copies of the appointment letters will be forwarded to Command Security Manager (B 054). Figures 2-5 and 2-6 contain sample appointment letters.

2004. SECURITY MANAGEMENT/SPECIAL SECURITY OFFICER COORDINATION

1. The appointed SSO is responsible for the operation of the Sensitive Compartmented Information Facility (SCIF) and the security, control, and utilization of Sensitive Compartmented Information (SCI) at this Base. Refer all matters relating to SCI or SSO requirements to the SSO.
2. Although the SSO runs the SCI program independently from the MCB Information and Personnel Security Program, there will be cooperation and coordination between the two, especially in regards to investigations and clearances. The SSO is responsible for initiating investigations for SCI clearances and access. The SSO will advise the CG MCB (B 054) that an investigation has been initiated by providing a copy of the investigation request as a tickler for the official record and advise the CG MCB (B 054) when results have been finally adjudicated. The CG MCB (B 054) in turn will keep the SSO advised of any information relating to an individual in the SCI Program or of changes to security policy and procedures that may impact an SCI Program.

2005. INTER-SERVICE SUPPORT AGREEMENTS (ISSA)

1. In that overall security aboard the MCB, Quantico is the responsibility of the CG MCB security servicing of various tenant activities will be performed pursuant to ISSA's. These services will be coordinated through the MCB Security Manager.
2. Tenant activity heads will keep the CG MCB (B 054) informed of any matters that may have a direct affect on the security procedures of this Base.

2006. COMMAND SECURITY PROCEDURES. Each activity aboard this Base and its tenant activities will publish written procedures specifying how the requirements of SECNAVINST 5510.30A, SECNAVINST 5510.36 and this manual will be accomplished. Necessary changes will be written as required to reflect changes in the activity's functions. Each activity's security procedures will specify the responsibilities of appointed security personnel and procedures to be followed for the control and handling of classified material. Partial guidelines for command security procedures are contained in chapter 2, Exhibit 2A of SECNAVINST 5510.36.

2007. EMERGENCY PLANS

1. Each activity that handles classified information will develop an emergency plan for the protection of classified material in case of natural disaster, civil disturbance, or enemy action. This plan must be detailed with specific procedures and responsibilities. Emergency destruction plans, if required, will be incorporated into the emergency plan. Accredited SCIF and designated Special Security Offices will include SCI emergency destruction plans as part of the organizational emergency plan.

2. In developing emergency plans, the guidance contained in chapter 2 exhibit 2B of SECNAVINST 5510.36 will be utilized.

2008. INSPECTIONS AND REVIEW

1. Commanding officers/directors are responsible for evaluating the effectiveness of the Information and Personnel Security Program within their organizations.

2. Inspections will be conducted by qualified personnel who will inquire into overall security management and procedures for classification management, accounting and control of classified information, physical protection of classified information, personnel security, and security education.

3. The Command Security Manager (B 054) will conduct two formal inspections annually, one scheduled announced and one spot inspection unannounced. Use exhibit 2A of this manual as a preparation guide.

4. Security inspections of areas where classified material is maintained will be conducted at the close of each working day by either the custodian or assistant custodian of classified material to ensure that all classified material (to include classified waste), is accounted for and properly stored in approved security containers, and that all such containers are locked. Additionally, all doors and windows will be secured. Standard Forms 701 and 702 (figures 2-7 and 2-8) will be utilized to record the fact that the inspection was conducted and by whom. For standardization purposes, all forms will have weekends and holidays highlighted in yellow and completed per the examples given. Also see paragraph 14008.

2009. UNANNOUNCED SECURITY INSPECTIONS

1. Unannounced after-hours security inspections are conducted periodically by security management personnel as an adjunct to existing security programs. These inspections are conducted to advise the CG MCB and activity heads of the real time security practices that exist aboard the Base. Unannounced security inspections may also be conducted during working hours at the direction of the Command Security Manager.

2. Prior to commencing an unannounced after-hours inspection, security management specialists will identify themselves to the duty officer/activity representative and request that the duty officer enter in their log the names of the inspection party, time inspection begins and ends, and the results thereof. The duty officer will accompany the inspection party on their inspection. Security specialists conducting the above inspections have instructions to:

a. Unlock and open for inspection such furnishings as desks, cabinets, lockers, and other containers not designated for storage of classified information, which could lead to compromise.

b. Check used carbon paper, typewriter ribbons, memo pads, floppy disks, and similar material for classified information.

c. Locate any classified material or information not properly safeguarded and deliver it to the duty officer in exchange for a receipt. The duty officer is responsible for taking appropriate measures to safeguard the classified material and correct security hazards discovered during the inspection.

3. Unannounced inspections conducted during normal working hours will be walk-through cursory examinations of office spaces to ensure that classified material is not left adrift or unattended and may include opening of safes for verification that unauthorized classified material is not being stored.
4. The inspection results will be recorded and forwarded to the activity head concerned by the Command Security Manager (B 054).
5. Organizations will correct discrepancies as soon as possible on all reported inspection results. Organizations are required to have on hand, all inspection report results and record the appropriate corrective action taken for the last 2 years.

2010. COUNTERINTELLIGENCE TECHNICAL ASSISTANCE. Security management personnel provide valuable assistance to activity heads in evaluating existing security programs or establishing requirements for a new security program. Specialists accomplish this task by conducting security surveys, evaluations, or courtesy inspections upon written request. These requests will be submitted to the CG MCB (B 054). In addition to the above services, Technical Surveillance Counter-measures inspections and Compromising Emanations inspections will be requested from the CG MCB (B 054) per the instructions contained in OPNAVINST C5510.93.

INFORMATION AND PERSONNEL SECURITY PROGRAM

(Letter Head)

5510
(Originator Code)
(Date)

From: Activity Head
To: Individual Appointee

Subj: DESIGNATION OF SECURITY MANAGER

Ref: (a) SECNAVINST 5510.30A
(b) SECNAVINST 5510.36
(c) MCBO 5510.1B

1. In compliance with the provisions of references (a), (b) and (c), you are designated as the Security Manager for (Unit/Activity).
2. You are directed to familiarize yourself with the duties of the Security Manager, utilizing paragraphs 2-3 and 2-4 of reference (a), paragraph 2-2 of reference (b), and reference (c) were applicable in the performance of your duties.
3. Previous appointments as Security Manager are revoked.

(SIGNATURE)

Copy to:
CG MCB (B 054)
Unit/Acty Scty Mgr

Figure 2-1.--Sample Security Manager Appointment Letter.

INFORMATION AND PERSONNEL SECURITY PROGRAM

(Letter Head)

5510

(Originator Code)

(Date)

From: (Unit/Organization)

To: Commanding General, Marine Corps Base (B 054) (Attn:
Head, Classified Material Control Center)

Subj: DESIGNATION OF AUTHORIZED RECIPIENTS FOR CLASSIFIED
MATERIAL

Ref: (a) SECNAVINST 5510.36

(b) MCBO 5510.1B

1. Per reference (a) and (b), the following persons whose specimen signatures appear below are authorized to receipt for classified material for _____ (Unit/Organization) up to and including the classification indicated.

<u>Name/Grade/SSN</u>	<u>Classification</u> <u>Authorized</u>	<u>Signature</u>
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

2. This certificate cancels and supersedes all previous certificates.

(SIGNATURE)

Copy to:
CG MCB (B 054)
Unit File

Figure 2-2.--Sample Designation of Authorized Recipients
Classified Material Letter.

INFORMATION AND PERSONNEL SECURITY PROGRAM

(Letter Head)

5510
(Originator Code)
(Date)

From: Activity Head
To: Individual Appointee

Subj: APPOINTMENT AS TOP SECRET CONTROL OFFICER

Ref: (a) SECNAVINST 5510.30A
(b) SECNAVINST 5510.36
(c) MCBO 5510.1B

1. In compliance with the provisions of reference (a), (b) and (c), you are appointed as the Top Secret Control Officer for (Unit/Activity).
2. You are directed to familiarize yourself with the duties of the Top Secret Control Officer utilizing paragraph 2-10 of reference (a), paragraph 2-3 of reference (b) and reference (c) were applicable in the performance of your duties.
3. Previous appointments as Top Secret Control Officer are revoked.

(SIGNATURE)

Copy to:
CG MCB (B 054)
Unit/Acty Scty Mgr

Figure 2-3.--Sample Top Secret Control Officer Appointment Letter.

INFORMATION AND PERSONNEL SECURITY PROGRAM

(Letter Head)

5510

(Originator Code)

(Date)

From: Activity Head

To: Individual Appointee

Subj: APPOINTMENT AS CLASSIFIED MATERIAL CUSTODIAN

Ref: (a) SECNAVINST 5510.30A

(b) SECNAVINST 5510.36

(c) MCBO 5510.1B

1. In compliance with the provisions of references (a) and (b), you are appointed as the Classified Material Custodian for (Unit/Activity).

2. You are directed to familiarize yourself with the duties of the Secondary Control Point Custodian utilizing paragraph 2-6.2 of reference (a) and paragraph 2003.3 of reference (b) and other directives as are required in the performance of your duties.

3. Previous appointments as Classified Material Custodian are revoked.

(SIGNATURE)

Copy to:

CG MCB (B 054)

Unit/Acty Scty Mgr

Figure 2-4.--Sample Secondary Control Point Custodian Appointment Letter.

INFORMATION AND PERSONNEL SECURITY PROGRAM

(Letter Head)

5510
(Originator Code)
(Date)

From: Activity Head
To: Individual Appointee

Subj: APPOINTMENT AS INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

Ref: (a) SECNAVINST 5239.3
(b) SECNAVINST 5510.36
(c) MCBO 5230.3

1. Per the references, you are hereby appointed as the Information Systems Security Officer for (Command/Activity).
2. You are directed to familiarize yourself with the duties of Information Systems Security Officer, and ensure compliance with all Information Assurance policies & procedures.
3. This letter supersedes all previous appointments.

(SIGNATURE)

Copy to:
CG MCB (B 054)
Unit/Acty Scty Mgr

Figure 2-5.--Sample Information Systems Security Officer
Appointment letter.

INFORMATION AND PERSONNEL SECURITY PROGRAM

(Letter Head)

5510
(Originator Code)
(Date)

From: Activity Head
To: Individual Appointee

Subj: APPOINTMENT AS INFORMATION SYSTEMS SECURITY COORDINATOR
(ISSC)

Ref: (a) SECNAVINST 5239.3
(b) SECNAVINST 5510.36
(c) MCBO 5230.3

1. Per the references, you are hereby appointed as the Information Systems Security Coordinator for (Command/Activity).
2. You are directed to familiarize yourself with the duties of Information Systems Security Coordinator, and ensure compliance with all Information Assurance policies & procedures.
3. This letter supersedes all previous appointments.

(SIGNATURE)

Copy to :
CG MCB (B 054)
Unit/Acty Scty Mgr

Figure 2-6.--Sample Information Systems Security Coordinator
Appointment Letter.

Figure 2-7.--Sample Activity Security Checklist.

2-16

[illegible]

Figure 2-8.--Sample Security Container Check Sheet.

EXHIBIT 2A
INFORMATION AND PERSONNEL SECURITY PROGRAM
INSPECTION CHECKLIST

The references key is as follows, SECNAVINST 5510.30A (PSP),
 SECNAVINST 5510.36 (ISP) and MCBO 5510.1B (MCBO IPSP).

YES NO N/A

- | | |
|-------------------------|--|
| _____

_____ | 1. Does the command hold the current edition of
SECNAVINST 5510.30A/SECNAVINST 5510.36?
MCBO P5510.1_ (ISP 1-1) (MCBO IPSP 1003.3) |
|-------------------------|--|

COMMAND SECURITY MANAGEMENT

- | | |
|-------------------------|--|
| _____

_____ | 2. Has the CO, (PSP 2-13 ISP 2-1) |
| _____

_____ | a. Approved an emergency plan for the protection
and destruction of classified information
(MCBO IPSP-2007) |
| _____

_____ | b. Ensured that the security manager and other
personnel have received security education and
training? (ISP-2003) (MCBO IPSP-2002/2003.3) |
| _____

_____ | c. Ensured that personnel are evaluated on the
handling, creation or management of classified
information on performance evaluation?
(SECNAVINST 5510.36 2-1.h) |
| _____

_____ | 3. To implement the ISP, has the CO designated in
writing a command? |
| _____

_____ | a. Security manager? (ISP 2-2 PSP 2-3) (MCBO
IPSP 2001.2) |
| _____

_____ | b. TSCO? (ISP 2-3 PSP 2-5) (MCBO IPSP 2001.2) |
| _____

_____ | c. Security assistant(s) and custodian(s)
(ISP 2-4 PSP 2-6) (MCBO IPSP 2001.2) |
| _____

_____ | d. One or more Contract Officer
Representatives (COR)? (ISP 2-6 PSP 2-7)
(MCBO IPSP 2001.2) |

YES NO N/A

- | | | | |
|-----|-----|-----|--|
| ___ | ___ | ___ | 4. Is the command's security manager named and identified to command personnel on command organizational charts, telephone listings, rosters, or other media? (ISP 2-2) (MCBO IPSP 4005) |
| | | | 5. Has the security manager: |
| ___ | ___ | ___ | a. Formulated, coordinated, and conducted a Security Education Program? (ISP 2-2 PSP 2-3) (MCBO IPSP 4000.3) |
| ___ | ___ | ___ | b. Kept command personnel abreast of all changes in security policies and procedures? (MCBO IPSP 2006) |
| ___ | ___ | ___ | c. Reported and investigated all security threats and compromises? (MCBO IPSP 19000) |
| ___ | ___ | ___ | d. Promptly referred all incidents, under their jurisdiction, to the NCIS? (MCBO IPSP 19001) |
| ___ | ___ | ___ | e. Developed security procedures for visitors who require access to classified information (MCBO IPSP 8000) |
| ___ | ___ | ___ | f. Does the security manager have direct and ready access to the appointing official? (PSP 2-3.2) |
| ___ | ___ | ___ | g. Does the security manager have sufficient authority and staff to function effectively? (PSP 2-3.3) |
| ___ | ___ | ___ | 6. Are personnel authorized to receipt for classified material also listed on at least one SF 700 envelope? (MCBO IPSP-2002.3) |
| ___ | ___ | ___ | 7. Are inspection reports on file? (MCBO IPSP 2009.6) |
| ___ | ___ | ___ | 8. Are discrepancies noted during inspections followed-up and corrected? (MCBO IPSP 2009.6) |

SECURITY EDUCATION

YES NO N/A

- | | | | |
|-----|-----|-----|--|
| ___ | ___ | ___ | 1. Does the command have an effective information Security Education Program? (ISP 3-1 PSP Chapter 4) (MCBO IPSP 4000) |
| | | | 2. Is additional ISP training provided to? |
| ___ | ___ | ___ | a. Derivative classifiers, security managers, and other security personnel? (ISP 3-3) (MCBO IPSP-4003) |
| ___ | ___ | ___ | b. Classified couriers? (MCBO IPSP-16012.6) |
| ___ | ___ | ___ | 3. Are orientation briefings given? (PSP 4-4) (MCBO IPSP 4003) |
| ___ | ___ | ___ | 4. Are annual refresher briefings given? (PSP 4-4) (MCBO IPSP 4003) |
| ___ | ___ | ___ | 5. Are counterintelligence briefings given? (PSP 4-4) (MCBO IPSP 4003) |
| ___ | ___ | ___ | 6. Are foreign travel briefings given? (PSP 4-4) (MCBO IPSP 4003) |
| ___ | ___ | ___ | 7. Have all personnel with NATO or SIOP-ESI or CNWDI access been briefed as required? (PSP 4-4) (MCBO IPSP 4003) |

PERSONNEL SECURITY

- | | | | |
|-----|-----|-----|--|
| ___ | ___ | ___ | 1. Are requests for PSI's kept to the minimum? (PSP 6-1) (MCBO IPSP 5000) |
| ___ | ___ | ___ | 2. Is the appropriate investigation being requested for access or assignment? (PSP 7-1) (MCBO IPSP 5000) |
| ___ | ___ | ___ | 3. Is there a program for continuous evaluation of eligibility for access or assignment to sensitive duties? (PSP 10-1) (MCBO IPSP 9002) |
| ___ | ___ | ___ | 4. Is access granted only to those with a need to know? (PSP 9-2) (MCBO IPSP 8000) |

YES NO N/A

- | | | | |
|-----|-----|-----|---|
| ___ | ___ | ___ | 5. Are personnel with established security clearance eligibility prohibited from gaining access to classified information until they have received an initial security briefing and signed a Standard Form 312, "Classified Information Nondisclosure Agreement"? (PSP 9-12) (MCBO IPSP 8003.3) |
| ___ | ___ | ___ | 6. Is access by foreign nationals or visitors adequately controlled? (PSP 11-3) (MCBO IPSP 10002) |
| ___ | ___ | ___ | 7. Do procedures ensure the Security Termination Statement is executed when required? (PSP 9-17) (MCBO IPSP 8003) |
| ___ | ___ | ___ | 8. Are military and civilian personnel made aware that they are subject to administrative sanctions for knowingly, willfully, or negligently committing security violations? (CH 1 SECNAVINST 5510) |
| ___ | ___ | ___ | 9. Are reports made to appropriate counterintelligence, investigative, and personnel security authorities concerning any employee who is known to have been responsible for repeated security violations? (PSP 3-2) (MCBO IPSP 3000) |
| ___ | ___ | ___ | 10. Are counterintelligence matters reported to NCIS when required? (PSP 3-2) (MCBO IPSP 3000) |
| ___ | ___ | ___ | 11. Have all personnel been advised of the requirement to report any contact with any individual regardless of nationality, in which unauthorized access is sought, or personnel are concerned that they may be the target of exploitation by a foreign entity? (PSP 3-3) (MCBO IPSP 3002) |

CLASSIFICATION MANAGEMENT

YES NO N/A

- | | | | |
|-----|-----|-----|--|
| ___ | ___ | ___ | 1. Is information classified only to protect NSI? (ISP 4-1) (MCBO IPSP 11000) |
| ___ | ___ | ___ | 2. Do procedures prohibit the use of terms such as "For Official Use only" or "Secret Sensitive" for the identification of classified information? (ISP 4-2) (MCBO IPSP 11001) |

MARKING

- | | | | |
|-----|-----|-----|--|
| ___ | ___ | ___ | 1. Are classified documents and their portions properly marked to include all applicable basic and associated markings? (ISP 6-1, 6-5) (MCBO IPSP 13000) |
| ___ | ___ | ___ | 2. Are originally classified documents marked with a "Classified by" and "Reason line? (ISP 6-8) |
| ___ | ___ | ___ | 3. Are derivatively classified documents marked with a "Derived from" line? (ISP 6-9) |
| ___ | ___ | ___ | 4. Is "Multiple Sources" annotated on the "Derived from" line of classified documents derived from more than one source? (ISP 6-9) |
| ___ | ___ | ___ | 5. Is a source listing attached to the file copy of all documents classified by "Multiple Sources?" (ISP 6-9) |
| ___ | ___ | ___ | 6. Are downgrading and declassification instructions included on all classified documents, less exception documents? (ISP 6-10) |
| ___ | ___ | ___ | 7. Are the appropriate warning notices placed on the face of classified documents? (ISP 6-11) |
| ___ | ___ | ___ | 8. Do documents, marked classified for training and test purposes, include a statement indicating that the documents are actually unclassified? (ISP 6-20) |
| ___ | ___ | ___ | 9. When removed or used separately, are component parts of classified documents marked as separate documents? (ISP 6-21) |

YES NO N/A

- ___ ___ ___ 10. Are electronically transmitted messages properly marked? (ISP 6-25)
- ___ ___ ___ 11. Are all classified materials such as AIS media, maps, charts, graphs, photographs, slides, recordings, and videotapes appropriately marked? (ISP 6-27 through 6-34)

SAFEGUARDING

- ___ ___ ___ 1. Does the command ensure that all DON employees (military and civilian) who resign, retire, separate, or are released from active duty, return all classified information in their possession? (ISP 7-1)
- ___ ___ ___ 2. Does the command have control measures in place for the receipt and dispatch of Secret information? (ISP 7-4) (MCBO IPSP 14003.2)
- ___ ___ ___ 3. Are control measures in place to protect unauthorized access to command TS, Secret, or confidential information (ISP 7-3, 7-4, 7-5) (MCBO IPSP 14003.3)
- ___ ___ ___ 4. Are working papers: (ISP 7-6), (MCBO IPSP 14004)
- ___ ___ ___ a. Dated when created?
- ___ ___ ___ b. Marked "Working Paper" on the first page?
- ___ ___ ___ c. Marked with the highest overall classification, center top and bottom, of each applicable page?
- ___ ___ ___ d. Destroyed when no longer needed?
- ___ ___ ___ e. Brought under accountability after 180 days or when they are released outside the command?
- ___ ___ ___ 5. Are SFs 703, 704, and 705 placed on all classified information when removed from secure storage? (ISP 7-9) (MCBO IPSP 14007.1)

YES NO N/A

- | | | | |
|-----|-----|-----|---|
| ___ | ___ | ___ | a. Are SFs 706, 707, 708, and 712 being utilized on all classified AIS media? (MCBO IPSP 14007.5) |
| ___ | ___ | ___ | b. Are classified typewriter ribbons, carbon sheets, plates, stencils, drafts, and notes controlled, handled, and stored per their classification level? (MCBO IPSP 14007.4) |
| ___ | ___ | ___ | 6. Has the command established procedures for end of day security checks, to include the use of SFs 701 and 702? (ISP 7-10) (MCBO IPSP 14008.1) |
| ___ | ___ | ___ | 7. Are entries made on the SF 702 form each and every time a security container, vault, or strong room is unlocked and locked? (MCBO IPSP 14008.2) |
| ___ | ___ | ___ | 8. Are classified vaults, secure rooms, and containers made an integral part of the end of day security check? (MCBO IPSP 14008.2) |
| ___ | ___ | ___ | 9. Are procedures in place to ensure that visitors have access only to information for which they have a need-to-know and the appropriate clearance level? (ISP 7-11) (MCBO IPSP 14009) |
| ___ | ___ | ___ | 10. Are procedures in place for classified meetings held at the command or hosted at cleared facilities? (ISP 7-12) (MCBO IPSP 14010) |

DISSEMINATION

- | | | | |
|-----|-----|-----|--|
| ___ | ___ | ___ | 1. Are special types of classified and controlled unclassified information disseminated per their governing instructions? (ISP 8-4) (MCBO IPSP 15000) |
| ___ | ___ | ___ | 2. Do all newly generated classified and unclassified technical documents include a distribution statement listed in exhibit 8A of SECNAVINST 5510.36? (ISP 8-7) (MCBO IPSP 15000.4) |

YES NO N/A

- ___ ___ ___ 3. Is command information intended for public release, including information released through AIS means (i.e., INTERNET, computer servers), submitted for pre-publication review? (ISP 8-8) (MCBO IPSP 15000.2)

TRANSMISSION AND TRANSPORTATION

- ___ ___ ___ 1. Is classified information transmitted and transported only per specific requirements? (ISP 9-2, 9-3, 9-4) (MCBO IPSP 16000)
- ___ ___ ___ 2. Are special types of classified information transmitted and transported per their governing instructions? (ISP 9-5) (MCBO IPSP 16004)
- ___ ___ ___ 3. Are command personnel advised not to discuss classified information over unsecured circuits? (ISP 9-6) (MCBO IPSP 16004)
- ___ ___ ___ 4. Are command procedures established for preparing classified bulky shipments as freight? (ISP 9-7) (MCBO IPSP 16008.2)
- ___ ___ ___ 5. Is classified information transported or transmitted outside the command receipted for? (ISP 9-10) (MCBO IPSP 16005)
- ___ ___ ___ 6. Does the command authorize the handcarry or escort of classified information, via commercial aircraft, only if other means are not available, and there is an operational need or contractual requirement? (ISP 9-11) (MCBO IPSP 16012.4)
- ___ ___ ___ 7. Are designated couriers briefed on their courier responsibilities and requirements? (ISP 9-11) (MCBO IPSP 16012.7)
- ___ ___ ___ 8. Are procedures established for the control and issuance of the DD 2501? (ISP 9-12) (MCBO IPSP 16012.7)

STORAGE AND DESTRUCTION

YES NO N/A

- | | | | |
|-----|-----|-----|---|
| ___ | ___ | ___ | 1. Are any command weaknesses, deficiencies, or vulnerabilities in any equipment used to safeguard classified information reported to the Command Security Manager? (ISP 10-1) (MCBO IPSP 17000) |
| ___ | ___ | ___ | a. Does the command ensure that weapons, money, jewelry or narcotics are not stored in security containers used to store classified information? |
| ___ | ___ | ___ | b. Does the command ensure that external markings on command security containers do not reveal the level of information stored therein? |
| ___ | ___ | ___ | 2. Does command security equipment meet the minimum standards of GSA? (ISP 10-2) (MCBO IPSP 17001) |
| ___ | ___ | ___ | 3. Does the command meet the requirements for the storage of classified bulky information? (ISP 10-3) (MCBO IPSP 17001) |
| ___ | ___ | ___ | 4. Are command vaults and secure rooms, not under visual control at all times during duty hours, equipped with electric, mechanical, or electro-mechanical access control devices? (ISP 10-7) (MCBO IPSP 17000) |
| ___ | ___ | ___ | 5. Are specialized security containers securely fastened to the structure, rendering them non-portable? (ISP 10-8) (MCBO IPSP 17001.4) |
| ___ | ___ | ___ | 6. Is classified information removed from designated work areas for work at home done so only with prior approval of appropriate officials? (ISP 10-10) (MCBO IPSP 14001.2) |
| | | | 7. Are command container combinations changed: (ISP 10-12) (MCBO IPSP 17002) |
| ___ | ___ | ___ | a. By individuals who possess the appropriate clearance level? |

YES NO N/A

- | | | | |
|-----|-----|-----|--|
| ___ | ___ | ___ | b. Whenever the container is first put into use? |
| ___ | ___ | ___ | c. Whenever an individual knowing the combination no longer requires access to the container (unless other sufficient controls exist to prevent access)? |
| ___ | ___ | ___ | d. Whenever a combination has been subjected to compromise? |
| ___ | ___ | ___ | e. Whenever the container is taken out of service? |
| ___ | ___ | ___ | 8. Are command container combinations marked, stored, and accounted for per the classification level of the information stored therein? (ISP 10-12) (MCBO IPSP 17002.3) |
| ___ | ___ | ___ | 9. Is there an SF 700, affixed inside each command security container? (ISP 10-12) (MCBO IPSP 17002.3) |
| ___ | ___ | ___ | 10. Does the SF 700 include the names, home addresses, and phone numbers of all persons having knowledge of the combination? (ISP 10-12) (MCBO IPSP 17002.3) |
| ___ | ___ | ___ | 11. Has the command established procedures for command key and padlock accountability and control? (ISP 10-13) |
| ___ | ___ | ___ | 12. Are command locks repaired only by authorized personnel who have been subject to a trustworthiness determination or who are continuously escorted? (ISP 10-15) (MCBO IPSP 17002.2) |
| ___ | ___ | ___ | 13. Are command security containers, previously placed out of service, marked as such on the outside and the "Test Certification Label" removed on the inside? (ISP 10-15) (MCBO IPSP 17001) |

YES NO N/A

- | | | | | |
|-----|-----|-----|-----|--|
| ___ | ___ | ___ | 14. | Are command security containers, with visible repair results, marked as such with a label posted inside the container stating the details of the repairs? (ISP 10-15)
(MCBO IPSP 17001) |
| ___ | ___ | ___ | 15. | Are all commercial IDSs used on command security containers, vaults, modular vaults, and secure rooms approved by the CNO (NO9N3)?
(ISP 10-16) (MCBO IPSP 17001) |
| ___ | ___ | ___ | 16. | Is command classified information destroyed when no longer required? (ISP 10-17)
(MCBO IPSP 17004.2) |
| ___ | ___ | ___ | 17. | Do all command shredders, pulverizes, and disintegrators meet the minimum requirements? (ISP 10-18) (MCBO IPSP 17005.2) |
| ___ | ___ | ___ | 18. | Are all command shredders, pulverizes, and disintegrators NOT meeting the minimum standards marked accordingly?
(MCBO IPSP 17005.2) |
| ___ | ___ | ___ | 19. | Has the command established effective procedures for the destruction of classified information? (ISP 10-19) (MCBO IPSP 17005) |
| ___ | ___ | ___ | 20. | When filled, are command burn bags sealed and safeguarded per the highest overall classification level of their contents?
(ISP 10-19) (MCBO IPSP 17006) |
| ___ | ___ | ___ | 21. | Is controlled unclassified information destroyed per the governing instructions?
(ISP 10-20) (MCBO IPSP 17007) |

INDUSTRIAL SECURITY PROGRAM

- | | | | | |
|-----|-----|-----|----|--|
| ___ | ___ | ___ | 1. | Has the command established an Industrial Security Program? (ISP 11-1) (MCBO IPSP 18000) |
| ___ | ___ | ___ | 2. | Has the commanding officer established or coordinated oversight over classified work carried out by cleared DoD contractor employees in spaces controlled or occupied at DON shore commands? (ISP 11-5)
(MCBO IPSP 18000.2) |

YES NO N/A

- | | | | |
|-----|-----|-----|---|
| ___ | ___ | ___ | 3. Have all Facility Access Determinations (FAD) been issued per SECNAVINST 5510.30A? (ISP 11-6) (MCBO IPSP 18005) |
| | | | 4. Does the command Contract Officer Representatives (COR): (ISP 11-8) (MCBO IPSP 18007) |
| ___ | ___ | ___ | a. Complete, issue, and sign all DD 254s? |
| ___ | ___ | ___ | b. Validate all contractor security clearances? |
| ___ | ___ | ___ | c. Verify Facility (Security) Clearance (FCLs) and storage capability prior to release of classified information? |
| ___ | ___ | ___ | d. Certify and approve all DD 1540s? |
| ___ | ___ | ___ | e. Provide additional security requirements? |
| ___ | ___ | ___ | f. Review all reports of industry security violations and forward to program managers? |
| ___ | ___ | ___ | g. Coordinate DD 254 reviews and guidance, as needed? |
| ___ | ___ | ___ | h. Verify that cleared DoD contractor employees who are used as couriers have been briefed on their courier responsibilities? (ISP 11-12) |
| ___ | ___ | ___ | 5. Is classified intelligence information disclosed only to those contractors cleared under the NISP? (ISP 11-14) |

LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

- | | | | |
|-----|-----|-----|--|
| ___ | ___ | ___ | 1. Since the last inspection, has the command had any incidents involving a loss or compromise of classified information? (ISP 12-1) (MCBO IPSP 19000) |
| ___ | ___ | ___ | 2. If a possible loss or compromise occurred, was a PI conducted? (ISP 12-4) (MCBO IPSP 19002) |

YES NO N/A

- | | | | | |
|-----|-----|-----|----|---|
| ___ | ___ | ___ | 3. | If a significant command weakness is identified, or a confirmed loss or compromise occurred, was a JAGMAN investigation conducted? (ISP 12-9) |
| ___ | ___ | ___ | 4. | When a loss or compromise of classified information or equipment has occurred, is appropriate investigative and remedial action(s) taken to ensure further loss or compromise does not recur? (ISP 12-14) |
| ___ | ___ | ___ | 5. | Is appropriate and prompt corrective action taken whenever a knowing, willful, or negligent compromise or repeated administrative disregard of security regulations occurs? (ISP 12-14) |
| ___ | ___ | ___ | 6. | Are procedures established for review of investigations by seniors? (ISP 12-14) |
| ___ | ___ | ___ | 7. | Are security reviews conducted on information subjected to loss or compromise? (ISP 12-15) |
| ___ | ___ | ___ | 8. | Are procedures established for classification reviews by originators or original classification authorities? (ISP 12-16) |
| ___ | ___ | ___ | 9. | Is receipt of improperly transmitted information reported to the sender? (ISP 12-19) |

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 3

COUNTERINTELLIGENCE MATTERS AND NATIONAL SECURITY

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	3000	3-3
FOREIGN TRAVEL	3001	3-3
COUNTERINTELLIGENCE.	3002	3-3
NATIONAL SECURITY POLICY	3003	3-3
MAINTENANCE PROCEDURES	3004	3-4

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 3

COUNTERINTELLIGENCE MATTERS AND NATIONAL SECURITY

3000. BASIC POLICY. Certain matters affecting national security must be reported to the Resident Agent, Naval Criminal Investigative Service (RA NCIS) so that counterintelligence measures can be taken. All Department of the Navy military and civilian personnel at Quantico, whether they have access to classified information or not, will report to their security managers, the Base Security Manager, the commanding officer or to the nearest command, any activities described below involving themselves, their immediate relatives, co-workers or others. These individuals will in turn immediately notify the RA, NCIS, Quantico or the Director, NCIS (DIRNAVCRIMINVSERV) Washington, DC by classified IMMEDIATE message, with Chief of Naval Operations (NO9N) as an information addressee.

a. Sabotage, espionage, international terrorism or deliberate compromise.

b. Personnel who possess a security clearance must report contacts with individuals seeking illegal access to classified materials.

c. Personnel who have access to classified information and commit or attempt to commit suicide.

d. Unauthorized absentees who have access to classified information.

e. Death or desertion of a DON person who has access to classified information.

3001. FOREIGN TRAVEL. Foreign travel briefings are normally provided by the RA, NCIS, MCB, Quantico prior to travel overseas.

3002. COUNTERINTELLIGENCE. Refer to chapter 3 of reference (a) for additional guidance on counterintelligence matters.

3003. NATIONAL SECURITY POLICY. Commanding officers are required to designate each national security position within their command per reference (a). Criteria for designating sensitive positions are contained in chapter 5 of reference (a).

3004. MAINTENANCE PROCEDURES. The Command Security Manager will maintain a record of position designation decisions using the format contained in exhibit 5A of reference (a). Reports will be filed in the Personnel Security Office.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 4

SECURITY EDUCATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	4000	4-3
RESPONSIBILITIES	4001	4-3
ASSISTANCE	4002	4-4
BRIEFINGS/MINIMUM REQUIREMENTS	4003	4-4
DEBRIEFINGS	4004	4-5
CONTINUING SECURITY AWARENESS	4005	4-6

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 4

SECURITY EDUCATION

4000. BASIC POLICY

1. The purpose of the Information and Personnel Security Program is to provide a framework for protection of information essential to national security, keeping it within authorized channels and away from hostile intelligence services.
2. The purpose of the Security Education Program is to ensure that all personnel at MCB, Quantico and its tenant activities understand the need to protect classified information and how to safeguard it. The goal is to develop fundamental habits of security to the point that proper discretion is automatically exercised in the discharge of duties, and security of classified information becomes a natural element of every task.
3. Each organization that handles classified information will establish and maintain an active Security Education Program to instruct all personnel, regardless of their position, rank, or grade, in the security policy and procedures.

4001. RESPONSIBILITIES

1. The CG MCB through the Command Security Manager is responsible for overall policy guidance, education requirements, and source support for the Security Education Program at this Base. This program will be designed to fit the particular requirements of the various groups of personnel who have access to classified information.
2. Although security managers may actually conduct the Security Education Programs from an operational standpoint, commanding officers, in keeping on line with other training programs, are responsible for ensuring that the Information and Personnel Security Training Programs mandated by SECNAVINST 5510.30A and SECNAVINST 5510.36 are also met.
3. The Naval Criminal Investigative Service (NCIS), division security managers, and all other security managers will provide necessary expertise and assistance as necessary to support commanding officers in their security training programs.

4. All automated information systems (AIS) and office automation (OA) personnel will be provided an appropriate security briefing upon arrival at the activity by the Information Systems Security Manager (ISSM) or designated representative per MCBO 5230.3.
5. Guidance to be used in the administration of the Security Education Program is contained in chapter 3 of SECNAVINST 5510.36.

4002. ASSISTANCE

1. Compliance with chapter 3 of SECNAVINST 5510.36 is of the utmost importance. A viable Security Education Program will eliminate problems and minimize the risk for security violations within the Information and Personnel Security Program.
2. To make the program work, security specialists are available to assist in the establishment of a Security Education Program and will provide limited training, as well as training aids upon request. Requests should be directed to the CG MCB (B 054) within 30 days prior to scheduled training.

4003. BRIEFINGS/MINIMUM REQUIREMENTS

1. Upon notification that a security clearance/access has been granted, each person who will have access to classified information will be given an **orientation briefing** by his or her security manager. The security manager will use a copy of the booklet "Command Security, A Security Awareness Orientation" for this purpose and then deliver it to the person being briefed.
2. Once a year all personnel who have access to classified information will receive a **refresher briefing**. The purpose is to enhance security awareness. It will include repetition of the requirement to report any contact with any citizen of a controlled country, hostile country, or any attempt by unauthorized persons to acquire classified information. Activity security managers will ensure that the refresher briefing is conducted in coordination with battalion S-2/3 officer, as appropriate.
3. Once every 2 years, those who have access to Secret or above information must attend a counterespionage briefing by an NCIS agent. The Command Security Manager will be responsible for the briefing arrangements with the NCIS. Special briefing arrangements with the NCIS can be made on a case-by-case basis. It is the responsibility of each organization that handles classified information to

establish and maintain an active Security Education Program to instruct all personnel, regardless of their position, rank, or grade, in current security policy and procedures. Each organization is further required to schedule, record and report annual and 2 year counterespionage briefings by name and date of attendees to the Command Security Manager (B 054), Personnel Security Office (PSO), for annotation on the master access roster.

4. Any individual that has had access to classified information and who plans to travel to or through a foreign country or to attend a meeting in the U.S. or elsewhere, in which representatives of foreign countries are expected to participate, will be given a foreign travel briefing. Foreign travel briefings will be made at least 5 working days prior to departure. Requests will be made to the NCIS via the Command Security Manager. Upon return, individuals will be debriefed as appropriate.

5. All personnel who require access to North Atlantic Treaty Organization (NATO)/Critical Nuclear Weapons Design Information (CNWDI) must have a final Secret clearance/access and submit a justification to and be briefed by the NATO/CNWDI control point officer or alternate on related security procedures before access is granted.

6. The special security officer is responsible for Sensitive Compartmented Information briefings.

4004. DEBRIEFINGS

1. Personnel having had access to classified information must be debriefed by their Command under the following conditions:

a. Prior to termination of active military service or civilian employment, or temporary separation for a period of 60 days or more, including sabbaticals and leave without pay.

b. At the conclusion of the access period when a limited access authorization has been granted.

c. When a security clearance is revoked for cause.

d. When a security clearance is administratively withdrawn.

e. When a member of the organization inadvertently has substantial access to information that they are not eligible to receive.

f. When a member having access to NATO/CNWDI information no longer requires access to such material the NATO/CNWDI Control Officer or alternate will debrief.

2. In all cases, commands will forward copies of all debriefing certificates/statements to the Command Security Manager (B 054), PSO.

4005. CONTINUING SECURITY AWARENESS. To enhance security in a continuing program, signs, posters, bulletins, e-mail notices, and plan of the day reminders are some of the methods that will be used to boost security awareness. The security manager shall be identified by name on command organizational charts, telephone listings, rosters, or other media.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 5

PERSONNEL SECURITY INVESTIGATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	5000	5-3
PERIODIC REINVESTIGATIONS.	5001	5-3
SUBMISSION OF PERSONNEL SECURITY QUESTIONNAIRES	5002	5-4
SENSITIVE POSITIONS	5003	5-4
CONTRACTOR PERSONNEL	5004	5-4
SECURITY MANAGERS.	5005	5-4
ELECTRONIC PERSONNEL SECURITY QUESTIONNAIRE (EPSQ)	5006	5-4
MAINTAINING QUESTIONNAIRE INFORMATION.	5007	5-5
RELEASE OF CLEARANCE INFORMATION . . .	5008	5-5

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 5

PERSONNEL SECURITY INVESTIGATIONS

5000. BASIC POLICY

1. No individual will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made regarding his/her loyalty, reliability, and trustworthiness. A Personnel Security Investigation (PSI) is conducted to gather information pertinent to these determinations.
2. Only commanding officers, the Command Security Manager and Special Security Officer (SSO) are authorized to request a PSI on individuals under their jurisdiction. Copies of a PSI submitted will be forwarded with receipts to the Command Security Manager (B 054) for entry into the computer bank/access rosters.
3. A PSI will not normally be requested for any individual who will be retired, resigned, or separated with less than 1 year of service remaining.
4. Investigations other than PSIs will be handled by the appropriate investigative agency (i.e. Naval Criminal Investigative Service, Criminal Investigations Division) and reported to the Command Security Manager when they impact assignments to sensitive positions or granting of a security clearance.
5. Further guidance concerning a PSI is contained in chapter 6 of reference (a).

5001. PERIODIC REINVESTIGATIONS (PR)

1. These types of reinvestigations will be submitted as follows:
 - a. PR (SCI/TS) are submitted 4 years and 6 months from date of last investigation.
 - b. Secret periodic reinvestigations are submitted 9 years and 6 months from date of last investigation.
 - c. Confidential periodic reinvestigations are submitted 14 years and 6 months from date of last investigation.

2. Special Access Programs (SAPs), Explosive Ordnance Disposal (EOD) team members and those personnel in Personnel Reliability Programs (PRP) will submit PRs at 4 years and 6 months from date of last investigation. Other requirements are contained in paragraph 6-8 of reference (a).

5002. SUBMISSION OF PERSONNEL SECURITY QUESTIONNAIRES

1. Personnel requiring security investigations may obtain assistance as follows:

a. Civilian personnel, contact the Command Security Manager (B 054).

b. Military personnel, contact your S2/S3 Officer at battalion level.

c. All others contact the Command Security Manager (B 054) MCB, Quantico.

2. All commanding officers/directors will ensure weekly audits of access rosters to ensure timely submission of PSIs.

5003. SENSITIVE POSITIONS. An Single Scope Background Investigation (SSBI) is required for each civilian employee of the DON appointed to a critical sensitive or special sensitive position. The Personnel Security Office (B 054) will be contacted for assistance in this matter.

5004. CONTRACTOR PERSONNEL. Investigative requirements for contractor personnel will be handled by the Personnel Security Office (B 054).

5005. SECURITY MANAGERS. All security managers must have a favorably adjudicated SSBI or PR completed within the past 5 years.

5006. ELECTRONIC PERSONNEL SECURITY QUESTIONNAIRE (EPSQ)

1. Electronic Personnel Security Questionnaires will be used by security personnel to submit PSIs.

2. Military and civilian personnel required to submit a PSI may download subject edition from the Defense Security Service (DSS) web site at: www.dss.mil. Once completed, validate and save subject edition to a diskette. Present the diskette to the Battalion S-2 Officer or the Command Security Manager (B 054), for transmission to the DSS or the office of Personnel Management (OPM). Finger print cards (when required) and signed release forms will be forwarded separately by security personnel.

5007. MAINTAINING QUESTIONNAIRE INFORMATION

1. S-2 Officers will provide one copy of completed PSIs for the members Service Record Book, the individual, and the Command Security Manager (B 054).
2. If an individual refuses to complete a required PSI after being advised of the effect of the refusal, terminate the PSI. Report the refusal to the Command Security Manager (B 054) for action as appropriate.
3. When an individual is separated, transferred or no longer needs the investigation, notify the Command Security Manager (B 054) so that the investigation can be canceled.

5008. RELEASE OF CLEARANCE INFORMATION. Active duty and civilian personnel leaving the U.S. Government service for employment with a U.S. Government contractor that requires a security clearance/access, may request a letter of verification of their most recent security clearance status from the Command Security Manager (B 054). Due to the Privacy Act of 1974 consideration, the Command Security Manager may only provide this information to the individual or to the contractor's Facility Security Officer upon formal written request by the individual.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 6

PERSONNEL SECURITY DETERMINATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	6000	6-3
RESPONSIBILITIES	6001	6-3
ADJUDICATIVE MATTERS	6002	6-4
PERSONNEL SECURITY DETERMINATION . . .	6003	6-4
FACILITY ACCESS DETERMINATIONS (FAD) PROGRAM.	6004	6-4
UNFAVORABLE DETERMINATION PROCESS. . .	6005	6-5
APPEALS.	6006	6-5
PERSONNEL SECURITY ACTIONS	6007	6-5

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 6

PERSONNEL SECURITY DETERMINATIONS

6000. BASIC POLICY. Guidance concerning personnel security determinations such as security clearance eligibility and assignments to sensitive duties is contained in chapter 7 of reference (a).

6001. RESPONSIBILITIES. The authority to determine access to classified information for MCB/MCCDC activities and tenants serviced by Inter-Service Support Agreements is vested in the Command Security Manager (B 054). The Command Security Manager will:

1. Control clearance and access to classified information for all assigned personnel on behalf of the commanding officer.
2. Request Personnel Security Investigations as appropriate.
3. Grant interim personnel security clearances per paragraph 8-5 of reference (a).
4. Maintain a personnel security record on all cleared personnel to include a record of security briefings and clearance/access determinations.
5. Certify security clearances (visit requests) for assigned personnel per chapter 11 of reference (a).
6. Administratively withdraw the access when the requirement for access to classified information no longer exists. Ensure debriefing statements are completed by battalion/division security managers and forwarded to the Command Security Manager (B 054). Notify Department of the Navy Central Adjudication Facility (DONCAF) that clearance and access are no longer required.
7. Authorize and limit access according to requirements, lower access authorized, when appropriate.
8. Continuously evaluate command personnel with regard to their eligibility for access to classified information, applying the standards contained in appendix F of reference (a). Notify the DONCAF when potential disqualifying information is developed.

9. Suspend an individual's access to classified information for cause when warranted and notify the DONCAF within 10 days.

10. Coordinate unfavorable personnel security determinations concerning personnel assigned to the various commands. Direct personnel to command assistance programs as appropriate. Assist affected personnel by explaining the personnel security determination process and provide personnel the command instructions provided with the Letter of Intent (LOI), Letter of Notification (LON), and Personnel Security Appeals Board (PSAB) notification letters.

11. Deny access and/or restrict admittance to command areas as deemed appropriate when disqualifying information regarding an individual from another command is revealed. Ensure the individuals parent command agency or facility is notified, to include the basis for that action.

6002. ADJUDICATIVE MATTERS

1. In view of the significance that each adjudication decision can have on a person's career, and to ensure the maximum degree of fairness and equity in these actions, the Command Security Manager and Battalion Commanding Officers/Security Managers will ensure compliance with the guidelines as set forth in paragraph 7-3 of reference (a).

2. Local reviews and adjudicative matters will be conducted by a civilian security manager GS-11 and above or a military officer/security manager.

6003. PERSONNEL SECURITY DETERMINATION. Commanding officers, Staff Judge Advocate, security officer, Provost Marshal, Substance Abuse Officer, Director of Human Resources, managers and supervisors will ensure that questionable or unfavorable information is made available to the Command Security Manager in the performance of his duties in making personnel security determinations per paragraph 7-4 of reference (a).

6004. FACILITY ACCESS DETERMINATIONS (FAD) PROGRAM

1. Chapter 7 of reference (a) provides guidance concerning contractor employees.

2. National Agency Checks for contractor employees may be submitted to Defense Security Service (DSS) per the above.

6005. UNFAVORABLE DETERMINATION PROCESS

1. Unfavorable personnel security determinations from or to DONCAF will be processed by the Command Security Manager. commanding officers, division directors, and the Director of Civilian Personnel will be kept informed on any action taken with regard to personnel under their administrative jurisdiction.

2. LOIs and other actions will be processed in such a manner as to ensure all deadlines are met and that the individual receives due process.

3. Paragraph 7-7 of reference (a) provides specific guidance for LOIs which will be coordinated through the Command Security Manager.

4. The Systems Security Officer (SSO) may process LOIs for those personnel having sensitive compartmented information access but will keep the Command Security Manager informed of the actions taken. This includes copies of correspondence, Electronic Personnel Security Questionnaires, and other correspondence documenting security actions taken.

6006. APPEALS. Appeals/personal appearances resulting from LOIs will be coordinated through the Command Security Manager (B 054). The Command Security Manager acts as the single focal point for MCB/MCCDC and outside agencies such as DONCAF and DSS.

6007. PERSONNEL SECURITY ACTIONS. When DONCAF forwards unfavorable personnel security actions, the Command Security Manager/SSO will, based upon their guidance:

1. Deny or revoke security clearance eligibility.
2. Deny or revoke special access authorization.
3. Deny or revoke assignments to sensitive duties.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 7

CLEARANCE

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	7000	7-3
CLEARANCE PROHIBITIONS	7001	7-3
RECORDING CLEARANCES	7002	7-3
INTERIM CLEARANCES	7003	7-3
UNIQUE SECURITY CLEARANCE REQUIREMENTS	7004	7-4
CLEARANCES UNDER THE NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP) . .	7005	7-4
CLEARANCE WITHDRAWAL OR ADJUSTMENT . .	7006	7-5
DENIAL OR REVOCATION OF A SECURITY CLEARANCE.	7007	7-5

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 7

CLEARANCE

7000. BASIC POLICY. Policy and guidance for the processing of security clearances is contained in chapter 8 of reference (a).

7001. CLEARANCE PROHIBITIONS. In addition to the prohibitions contained in paragraph 8-3 of reference (a), clearances will not normally be requested for:

1. Generals' drivers (aide will handle classified material; drivers will handle vehicles)
2. Unescorted access for sake of convenience in classified areas.
3. Mail Orderlies, except for classified couriers.
4. Permanent access when temporary clearances will do.

7002. RECORDING CLEARANCES

1. A copy of the Department of Navy Central Adjudication Facility (DONCAF) certification message will be maintained in each Officer Qualification Record and enlisted Service Record Book per paragraph 8-4 of reference (a).
2. A copy of the certification message will be retained in the files of the Command Security Manager (B 054).

7003. INTERIM CLEARANCES

1. The Command Security Manager will grant interim clearances for MCB/MCCDC and tenant activity personnel based upon the guidance set forth in chapter 8 of reference (a).
2. Interim clearances will be recorded on OPNAV 5510/413, Personnel Security Action Request. Copies will be forwarded to battalion commanding officers for record purposes.
3. Division security managers will audit weekly access rosters provided by the Command Security Manager (B 054) to ensure tracer action is completed for interim clearances over 6 months old.

4. The Command Security Manager will withdraw an interim clearance upon receipt of a Letter of Intent, and suspend access per paragraph 9-18 of reference (a).
5. Failure to comply with Personnel Security Investigation submission requirements will result in withdrawal of interim clearances.

7004. UNIQUE SECURITY CLEARANCE REQUIREMENTS

1. Every commanding officer must have a favorably adjudicated Single Scope Background Investigation (SSBI) and the security clearance equivalent to the highest level of classified information maintained at the command. The incumbent commanding officer will review the records of the prospective commanding officer to ensure that the individual has the necessary investigation and security clearance certification to assume command. When the prospective command does not have the appropriate security clearance certification of SSBI, the incumbent will ensure the necessary requests for certification and/or investigation are submitted.
2. Navy and reserve personnel security clearances will be coordinated through the Command Security Manager.
3. Clearances for consultants to government contracting activities will be processed by the Command Security Manager.

7005. CLEARANCES UNDER THE NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP)

1. Under normal circumstances, contractor clearances will be processed by the contractor's Facility Security Officer. However, when questions arise, the Command Security Manager will act as the focal point to resolve security clearance issues.
2. Adverse or questionable information which concerns a cleared contractor employee assigned to a worksite under the control of MCB/MCCDC or one of its tenants will be reported to the Command Security Manager, who in turn will report to Defense Security Service Operation Center Columbus. The Systems Security Officer (SSO) will keep the Command Security Manager informed when sensitive compartmented information (SCI) is involved.

7006. CLEARANCE WITHDRAWAL OR ADJUSTMENT

1. Although clearances remain in effect, division security managers will debrief their personnel upon transfer out of their Division. OPNAV 5511/14 Security Termination Statement will be used and forwarded to the Command Security Manager. In turn, this action will alert security personnel to remove the individual from Base access rosters or make corrections as appropriate. It is imperative that OPNAV Form 5511/14 be executed and forwarded in a timely manner.

2. The administrative withdrawal or downgrading of a security clearance or access is authorized when prompted by developed derogatory information. On behalf on the commanding officer, the Command Security Manager may suspend the individual's access for cause and will report the suspension and/or the derogatory information to the DONCAF. The suspension of access must be accomplished per paragraph 9-18 of reference (a). The SSO will coordinate this action when SCI access is an issue. When access is suspended, the clearance certification must be removed from the individual's service record.

7007. DENIAL OR REVOCATION OF A SECURITY CLEARANCE

1. DONCAF grants all security clearances. Commands are responsible for ensuring that the DONCAF is apprised of any information that suggests an individual should have his/her clearance denied or revoked. The Command Security Manager will act as the focal point in these matters, overseeing the continuous evaluation program to ensure due process is given to all personnel affected.

2. Commanding officer's, Provost Marshals Office, (PMO) Office of the Staff Judge Advocate (SJA), and the Command Substance Abuse Center (CSAC) personnel will provide adverse information to the Command Security Manager in order to reinforce the commands continuous evaluation program.

3. Letters of intent and other security related information bypassing the Command Security Manager should be turned over to him as pertaining to a matter under his cognizance. The Command Security Manager will ensure that proper procedures and follow up are completed in the times prescribed.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 8

ACCESS TO CLASSIFIED INFORMATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	8000	8-3
GRANTING ACCESS TO CLASSIFIED INFORMATION.	8001	8-3
REQUESTING ACCESS.	8002	8-3
TERMINATION OF ACCESS.	8003	8-4
INVESTIGATION.	8004	8-4
ACCESS ROSTERS	8005	8-4
ACCESS FOR PERSONNEL OTHER THAN PERMANENT PERSONNEL.	8006	8-5
SUSPENSION OF ACCESS	8007	8-5
ACCESS TO AND DISSEMINATION OF RESTRICTED DATA (RD) INCLUDING CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI).	8008	8-6
FIGURE		
8-1 Sample Letter Requesting Access to Classified Material .		8-7
8-2 Sample Records Check.		8-9
8-3 Sample Nondisclosure Agreement.		8-10
8-4 Sample Security Termination Statement		8-12

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 8

ACCESS TO CLASSIFIED INFORMATION

8000. BASIC POLICY

1. Access to classified information will be limited to the minimum number of individuals necessary to accomplish the mission and will be based upon "need to know". Level of access will be restricted to the minimum level required. Per paragraph 9-1 of reference (a), no one will be granted access based upon rank, position, or clearance.
2. A Classified Information Nondisclosure Agreement (SF 312) will be executed by all persons requesting access.
3. Command/division security managers will ensure that personnel under their jurisdiction are briefed per paragraph 4-5 of reference (a) prior to granting access.

8001. GRANTING ACCESS TO CLASSIFIED INFORMATION

1. While the commanding officer has ultimate authority over those who have access, it is the Command Security Manager who must implement the process to ensure fairness, uniformity in the program and due process. It is extremely important that they work as one.
2. Access involving Sensitive Compartmented Information (SCI) issues may be granted per paragraph 9-3 of reference (a). The Systems Security Officer (SSO) must include the Command Security Manager in the administrative aspects of the program. Copies of Electronic Personnel Security Questionnaires (EPSQ), clearance certifications, denials and revocations must be forwarded to the Command Security Manager so that access rosters, security records, and other matters are promptly updated.

8002. REQUESTING ACCESS

1. The ultimate authority for granting access to classified information rests with the CG MCB thru the Command Security Manager, who is responsible for the security of the information and materials of this Base. The Command Security Manager will grant access to classified information to an individual who has official "need to know", meets eligibility requirements, and has no locally available disqualifying information.

2. The authority of the Command Security Manager to grant access to classified information is subject to the restrictions as set forth in paragraph 9-2 of reference (a).

3. A letter requesting access to classified information for permanent personnel will be prepared utilizing the format outlined in figure 8-1. Each request will contain the job title, a brief job description and complete justification (to include who, what, why, when, and where) of the "need-to-know", so that fair and proper adjudication of the request can be made to grant or deny access. A standard in the performance of duties or job description is not sufficient justification. In compliance with current regulations, a local records check (MCB Form 5511/16 (figure 8-2) will be enclosed with the letter request. Adverse information will be forwarded by separate correspondence to the CG MCB, Attn: Command Security Manager. A Classified Information Nondisclosure Agreement (SF 312) (figure 8-3) will be enclosed. If North Atlantic Treaty Organization (NATO)/Critical Nuclear Weapon Design Information (CNWIDI) access is requested, a final Secret clearance must be granted and a brief conducted by the Command Security Manager (B 054 NATO Control Point Officer).

8003. TERMINATION OF ACCESS. Request for termination of access on Base permanent personnel will be submitted in writing (figure 8-4) by activity heads to the CG MCB (B 054) per paragraph 9-17 of SECNAVINST 5510.30A.

8004. INVESTIGATION. Should a request for access reveal the need for an investigation/reinvestigation to qualify subject for a clearance/access, commanding officers/directors will direct personnel to the Battalion S-2 (military), Security Manager's Office (civilians), or the SSO (SCI) as appropriate. An EPSQ will be processed with copies forwarded to the Command Security Manager (B 054).

8005. ACCESS ROSTERS. The Command Security Manager maintains and distributes a weekly military, civilian, and visitor access roster. These rosters serve several purposes, so it is imperative that all security managers audit the rosters and submit changes to the Command Security Manager (B 054) in a timely manner.

8006. ACCESS FOR PERSONNEL OTHER THAN PERMANENT PERSONNEL

1. The Commanding Officer, Marine Helicopter Squadron-one (HMX-1) will be responsible for processing PSIs and the subsequent granting, denying, or terminating of security clearances for personnel within the organization.
2. Access for attached service personnel will be processed by the Command Security Manager (B 054).
3. Student access will be requested by the cognizant school director. The letter requesting access for each class will be accompanied by an alphabetized student class roster, Local Records Check, and SF 312 for each student.

8007. SUSPENSION OF ACCESS

1. When questionable or unfavorable information becomes available concerning an individual who has been granted a clearance/access, the commanding officer may decide to suspend access. Suspension of access for cause may only be used as a temporary measure until the individual's eligibility for access has been resolved and prior to transferring an individual to a different command. Suspension of access will be based upon the criteria as set forth in paragraph 9-18 of reference (a).
2. When effecting suspensions of access, commanding officers, working with the Command Security Manager must:
 - a. Comply with the provisions of paragraph 9-18 of reference (a).
 - b. Notify the Command Security Manager (B 054), division director, or activity head of the suspension actions taken against the individual under their charge.
 - c. Take steps to ensure that the individual's name is removed from all local access rosters, and that co-workers are notified of the limitations of suspensions.
 - d. Ensure the combinations to classified storage containers to which the individual has access are changed.
 - e. Post a notice of suspension of access in the individuals personnel file, pending resolution of the individual's eligibility status.

8008. ACCESS TO AND DISSEMINATION OF RESTRICTED DATA (RD) INCLUDING
CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)

1. Access to RD/CNWDI will be requested and processed by the Command Security Manager per paragraph 9-19 of reference (a).
2. Requests for access and approval to RD at other DoD facilities will be made utilizing the Department of Energy Visit Request form 5631.20. Division security managers may prepare the form for the Command Security Manager or Assistant Security Managers signature, which are the DoD certifying officials identified in DoD 5210.2.

INFORMATION AND PERSONNEL SECURITY PROGRAM

LETTER HEAD

5510
(Originator Code)
(Date)

From: Activity Head
To: Commanding General, Marine Corps Base, Quantico (B 054)
Via: (Applicable Division Directors/Battalion Commander)

Subj: REQUEST FOR ACCESS TO CLASSIFIED MATERIAL IN THE CASE OF
(GRADE/RATING, FULL NAME, SSN AND COMPONENT)

Ref: (a) MCBO 5510.1B

Encl: (1) Local Records Check (MCB Form 5511/16 (12/90))
(2) NATO/CNWDI Briefing Statements/Debriefing Statement
(if required)
(3) Classified Information Nondisclosure Agreement
(SF 312)
(4) Attestation Statement

1. Per the reference, it is requested that the subject named individual be granted access to classified material inclusive to (show level of access required). Subject requires this access to perform duties as a (billet title). Briefly justify using guidelines listed below.

- a. Does the individual really have a need to know?
- b. Who is the individual replacing? (Was clearance terminated?)
- c. Is access required on a routine basis? (If not, access will normally be denied or a temporary clearance may be granted.)
- d. Has the individual been here for a lengthy period of time, never had access, and suddenly thinks it is necessary to preclude losing a clearance?
- e. Is there another person who already has access that can handle the workload?

Figure 8-1.--Sample Letter Requesting Access to Classified Material.

Subj: REQUEST FOR ACCESS TO CLASSIFIED MATERIAL IN THE CASE OF
(GRADE/RATING, FULL NAME, SSN AND COMPONENT)

f. Do not describe billet - Describe need for classified access
(i.e. description of classified project, participation in continued
classified period of instruction, etc.)

2. It is understood that access to classified material is based on a
strict "need to know" basis and access requests are to be kept at a
minimum.

3. As required by the reference, enclosures (1) through (4) are
attached. (Enclosure (1) is conducting a local records check (LRC)
on the subject named individual. It is requested that the applicable
organizational commander initiate the LRC in compliance with the
reference.)

SIGNATURE

Figure 8-1.--Sample Letter Requesting Access to Classified
Material - Continued.

INFORMATION AND PERSONNEL SECURITY PROGRAM

LOCAL RECORDS CHECK

MCCDC 5511/16 (12/90) FPP 33571

Date _____

NAME (Last, First, Middle)	Social Security No.	Rank	MOS
Command/Unit	Pay Entry Base Date	Date of Birth	
Place of Birth (City, County, State)	Citizenship	Date Naturalized	
Marital Status <input type="checkbox"/> Married <input type="checkbox"/> Single	Name of Spouse	Citizenship of Spouse	
Investigative Basis	Date Investigation Completed	Investigative Agency	
Level Clearance (FOR SCTY MGR'S USE ONLY)	Clearance Status <input type="checkbox"/> Final <input type="checkbox"/> Interim <input type="checkbox"/> Temporary	Date Clearance Issued	

REMARKS:

1. Medical Officer/Commanding Officer/Personnel Officer — **DO NOT** summarize adverse/derogatory information on this form. All such information should be submitted to the Commanding General (C 054) Attn: Security Manager, by separate correspondence. Verifying Officer, verify above except for level of clearance information prior to submission to Commanding General.

2. **MEDICAL OFFICER.** Review the individual's medical records. Check the appropriate box, sign the form and return to the Commanding Officer of the Organization shown above.

- ☐ a. No adverse/derogatory information.
- ☐ b. Adverse/derogatory information. Date Forwarded _____
- ☐ c. Temporary medical record checked with ☐ no adverse/derogatory information ☐ adverse/derogatory information revealed in record. (In remarks indicate circumstances surrounding loss/non-availability of original record.)

Signature _____

3. **COMMANDING OFFICER/DIRECTOR, CIVILIAN PERSONNEL.** Complete the above clearance information after reviewing OQR/SRB/Personnel File (UPB, Unit Diary and other available records). Check appropriate box and forward with request for access to Commanding General (C 054) Attn: Security Manager. Upon Commanding General's receipt, a letter will be returned approving or denying clearance/access. If clearance/access is approved, make appropriate entry in the Manpower Management System (MMS).

- ☐ a. No adverse/derogatory information in OQR/SRB/Personnel File.
- ☐ b. Adverse/derogatory information. Date Forwarded _____

Signature _____

4. POLICE RECORDS CENTRAL FILES:

(Military Police/Security Manager/Counterintelligence records check.)

- ☐ a. No adverse/derogatory information.
- ☐ b. Adverse/derogatory information. Date Forwarded _____

Signature _____

Figure 8-2.--Sample Records Check.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

AND THE UNITED STATES

(Name of Individual — Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable

312-102

STANDARD FORM 312 (Rev. 1-00)
Prescribed by NARA/ISCO
32 CFR 2003. E.O. 12958

Figure 8-3.--Sample Nondisclosure Agreement.

INFORMATION AND PERSONNEL SECURITY PROGRAM

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958, Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b) (8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)
ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)		

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS (Type or print)		NAME AND ADDRESS (Type or print)	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (Rev. 1-00)

Figure 8-3.--Sample Nondisclosure Agreement - Continued.

INFORMATION AND PERSONNEL SECURITY PROGRAM

SECURITY TERMINATION STATEMENT

OPNAV 5511/14 (REV. 7-78)
S/N 0107-LF-055-1171

*Enter name and address of appropriate Naval or
Marine Corps activity obtaining statement.*

1. I HEREBY CERTIFY that I have conformed to the directives contained in the Information Security Program Regulation (OPNAV Instruction 5510.1), and the Communications Security Material System Manual (CMS-4) in that I have returned to the Department of the Navy all classified material which I have in my possession.

2. I FURTHER CERTIFY that I no longer have any material containing classified information in my possession.

3. I shall not hereafter communicate or transmit classified information orally or in writing to any unauthorized person or agency. I understand that the burden is upon me to ascertain whether or not information is classified and agree to obtain the decision of the Chief of Naval Operations or his authorized representative on such matters prior to disclosing information which is or may be classified.

4. I will report to the Federal Bureau of Investigation or to competent naval authorities without delay any incident wherein an attempt is made by an unauthorized person to solicit classified information.

5. I, _____, have been informed and am aware that Title 18 U.S.C., Sections 793-799, as amended and the Internal Security Act of 1950 prescribe severe penalties for unlawfully divulging information affecting the National Defense. I certify that I have read and understand appendix F of the Information Security Program Regulation OPNAV Instruction 5510.1. I have been informed and am aware that certain categories of Reserve and Retired personnel on inactive duty can be recalled to duty, under the pertinent provisions of law relating to each class for trial by court-martial for unlawful disclosure of information. I have been informed and am aware that the making of a willfully false statement herein renders me subject to trial therefor, as provided by Title 18 U.S.C. 1001.

6. I have/have not received an oral debriefing.

SIGNATURE OF WITNESS	SIGNATURE OF EMPLOYEE OR MEMBER OF NAVAL OR MARINE CORPS SERVICE (Fill in first, middle, and last name If military, indicate rank or rate. If civilian indicate grade.)
TYPE OR PRINT NAME OF WITNESS	DATE

Figure 8-4.--Sample Security Termination Statement.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 9

CONTINUOUS EVALUATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	9000	9-3
COMMAND REPORTS OF LOCALLY DEVELOPED UNFAVORABLE INFORMATION	9001	9-3
CONTINUOUS EVALUATION	9002	9-4

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 9

CONTINUOUS EVALUATIONS

9000. BASIC POLICY. Commanding officers/directors and their security managers are responsible for establishing and administering a program of continuous evaluation to ensure personnel with clearances/access and those assigned to sensitive positions are an acceptable security risk. Under this program, they must establish internal channels for reporting information reflecting on an individual's loyalty, reliability, judgment, and trustworthiness so that it may be assessed from a security perspective. There should be complete understanding by the personnel officer, security officer, security manager, legal officer, medical officer, Command Substance Abuse Center Officer, and supervising personnel that information which could place an individual's loyalty, reliability, judgment, and trustworthiness in question must be evaluated for a security standard. They should be familiar with the continuous evaluation check sheet, exhibit 10A, of reference (a) and the adjudication guidelines contained in appendix G of reference (a), and alerted that bad behavior indicating unexplained affluence, financial instability, alcohol and drug abuse, mental or emotional instability, or criminal conduct is potentially significant to an individual's security status. Activities should act to identify problem areas at an early stage and to direct personnel to programs designed to counsel and assist them when they are experiencing financial, emotional, or medical difficulties.

9001. COMMAND REPORTS OF LOCALLY DEVELOPED UNFAVORABLE INFORMATION

1. Co-workers have an equal obligation to advise their supervisor or appropriate security official when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

2. When derogatory or questionable information is acquired on an individual who is eligible for or holds a security clearance or special access authorization or who is assigned to a sensitive position, it is forwarded to the Command Security Manager who must reevaluate that individual's eligibility for access or assignment. Activity heads must make a determination upon initial receipt of credible derogatory information whether to suspend eligibility/access to classified information and/or continue assignment to a sensitive position and then notify the Command Security Manager.

Activity heads must make a determination upon initial receipt of credible derogatory information whether to suspend eligibility/access to classified information and/or continue assignment to a sensitive position and then notify the Command Security Manager.

3. Supervisors will comment on the continued security clearance eligibility of subordinates who have access to classified information in conjunction with regularly scheduled performance appraisals. See paragraph 10-4 of reference (a) for guidance.

4. Patterns of foreign travel by cleared personnel, or their failure to report such travel in advance as required, may have counterintelligence implications. A report of such travel will be referred to the Command Security Manager.

9002. CONTINUOUS EVALUATION

1. When questionable or unfavorable information, as identified in appendix F of reference (a), becomes available concerning an individual who has been granted access to classified information or assigned to a sensitive position, commands will report that information to the Command Security Manager for reporting to the Department of Navy Central Adjudication Facility (DONCAF). Commands will report all information, which meets the appendix F standards without attempting to apply or consider any mitigating factors that may exist. Use of exhibit 10A of reference (a) is encouraged to ensure that there is sufficient information upon which to base a determination.

2. If the Command Security Manager determines that the developed information is significant enough to require a suspension of the individual's access for cause, the suspension action will be accomplished per paragraph 9-18 of reference (a) using the proper administrative chain of command.

3. Sensitive compartmented information (SCI) access will be suspended by the Systems Security Officer (SSO), Marine Corps Intelligence Activity per reference (a) and Director Central Intelligence Directive regulations. The SSO will coordinate these activities with the Command Security Manager.

4. A command report of suspension of access for cause will automatically result in suspension of the individual's clearance eligibility by the DONCAF. Once clearance eligibility is suspended

(or the individual is debriefed from SCI access for cause), the individual may not be granted access or considered for re-indoctrination into SCI access until clearance eligibility has been reestablished by the DONCAF.

5. The Command Security Manager will act as the liaison in matters involving the DONCAF, except in those instances where the SSO is required to go direct.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 10

VISITOR ACCESS TO CLASSIFIED INFORMATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY.	10000	10-3
VISIT REQUEST	10001	10-3
FOREIGN VISITS.	10002	10-4
VISITS TO FOREIGN COUNTRIES	10003	10-5

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 10

VISITOR ACCESS TO CLASSIFIED INFORMATION

10000. BASIC POLICY

1. The term visitor applies as follows:

a. A visitor to MCB/MCCDC and its tenants is any person who is not attached to or employed by the activity or staff.

b. A person on temporary additional duty is considered a visitor. Personnel on temporary duty orders, reservist on active duty for training or those personnel assigned on a quota to a school or course of instruction are considered as visitors when not attached to this Command.

c. Cleared DoD contractors are considered as visitors.

2. Commanding officers and directors will establish procedures to ensure that only visitors with an appropriate level of security clearance and need to know are granted access to classified information. If an escort is required for the visitor, a properly trained military or civilian member or a contractor assigned to the Command may be used. The activity receiving the visitor is responsible for ensuring that the visitor has proper identification. An ID card will include a recent and recognizable photograph, the name, and social security number of the bearer. Military/civilian and contractor ID cards, or a valid drivers license containing all of the above elements may be used. Report any attempt to gain access to classified information by persons using fraudulent IDs to the Command Security Manager, or to the Naval Criminal Investigative Service (NCIS).

3. When the commanding officer permits a visit on an unclassified basis by the general public, a written statement of command safeguards will be prepared and implemented to address the possibilities of the presence of foreign agents among the visitors.

10001. VISIT REQUEST

1. All visit requests to or from MCB/MCCDC and tenant commands will be in compliance with paragraph 11-2 of reference (a). Incoming visit requests should be addressed to the Command Security Manager

Attn: Visitor Control. It is extremely important that visit requests contain the name of the activity to be visited and point of contact so that the Command Security Manager can forward the request on time after validation.

2. The Special Security Officer (SSO) does not process collateral visit requests. Therefore, do not submit visit requests through back channels unless they are sensitive compartmented information related.

3. Visitor clearance procedures discussed in this chapter should not be confused with area clearances required for entrance into a foreign country.

4. Under no circumstances will personnel hand carry their own visit requests to the places being visited. Hand carried orders do not contain the required information and therefore, cannot be used in lieu of visit requests.

10002. FOREIGN VISITS

1. SECNAVINST 5510.34, manual for the Disclosure of Department of Navy Military Information to Foreign Governments and International Organizations, 4 Nov 93 (NOTAL), and SECNAVINST 5510.30A provide guidance on foreign nationals and representatives of foreign entities.

2. Foreign visits are handled through the Visitor Control Coordination Center, G-3 (Operations Division), MCB. Visitor Control will coordinate visits involving technical discussions or the disclosure of classified material through the Command Security Manager to ensure approval of these visits by the Navy International Programs Office, the Commandant of the Marine Corps and the NCIS in matters involving security issues.

3. Receipt of a fraudulent visit request will be reported to the nearest NCIS Office and to the Command Security Manager (B 054).

4. Visits involving access to and dissemination of Restricted Data, or to facilities of the Department of Energy, are governed by the policies and procedures in DoD 5210.2, Access To and Dissemination of Restricted Data, 12 Jan 78 (NOTAL). The Command Security Manager's Office will sign, U.S. Department of Energy, Request for Visit or Access Approval Form DOE F 5631.20.

5. Visits involving access to and dissemination of Sensitive Compartmented Information are governed by the SSO, Marine Corps Intelligence Activity, and the procedures contained in Director Central Intelligence Directive.

6. Visit requests may be transmitted by facsimile, message or by electronic mail. When transmitted by facsimile, the visit request must be on official letterhead stationery. OPNAV form 5521/27 may also be used provided it is completed in its entirety.

NOTE: When visit requests are sent by facsimile regardless of which format is utilized the unit security manager or equivalent authority must **sign** those requests.

10003. VISITS TO FOREIGN COUNTRIES

1. Commanding officers and directors proposing sponsorship of an official visit to a foreign country will note the requirements of chapter 11 of SECNAVINST 5510.30A.

2. Visits to foreign countries in which classified information is involved will be coordinated through the Command Security Manager.

3. Foreign travel briefs will be conducted by NCIS. Level I force protection briefs will be given as required.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 11

CLASSIFICATION MANAGEMENT

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	11000	11-3
CLASSIFICATION DESIGNATIONS	11001	11-3
CLASSIFICATION GUIDANCE	11002	11-4
OCA TRAINING	11003	11-4
DERIVATIVE CLASSIFICATION	11004	11-5
ACCOUNTABILITY OF CLASSIFIERS.	11005	11-5
FOREIGN GOVERNMENT INFORMATION (FGI)	11006	11-5
SYSTEMATIC REVIEWS	11007	11-6
CONTINUED PROTECTION GUIDELINES	11008	11-6
REQUESTS FOR MANDATORY DECLASSIFICATION REVIEW	11009	11-6
DECLASSIFICATION, DOWNGRADING, AND UPGRADING.	11010	11-6

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 11

CLASSIFICATION MANAGEMENT

11000. BASIC POLICY

1. Executive Order 12958 is the prime basis for classifying information except as provided in the Atomic Energy Act of 1954, as amended. In keeping with the policy of the DON to make available to the public as much information as possible concerning its activities information at MCB, Quantico will be classified only to protect national security.

2. Unnecessary or higher than necessary classification will be avoided. If there is reasonable doubt about the need to classify information, it shall not be classified. When there is reasonable doubt about the appropriate level of classification, safeguard the information as if it were classified at the higher level until an original classification authority (OCA) makes a determination. This determination must be made within 30 days. (chapter 4, SECNAVINST 5510.36)

11001. CLASSIFICATION DESIGNATIONS. Information which requires protection against unauthorized disclosure in the interest of national security must be classified in one of three designations: "Top Secret," "Secret," or "Confidential." The markings "For Official Use Only," and "Limited Official Use" cannot be used to identify classified information, nor can you use modifying terms in conjunction with authorized classification designations, such as "Secret Sensitive."

1. Top Secret is the designation applied only to information the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to national security. The CG MCCDC and the Commander Marine Corps Systems Command (COMMARCORSSYSCOM) are the only DON officers designated to exercise Top Secret OCA aboard MCB, Quantico.

2. Secret is the designation applied only to information the unauthorized disclosure of which could reasonably be expected to cause serious damage to national security. The CG MCCDC and the COMMARCORSSYSCOM are the only DON officials designated to exercise Secret OCA aboard MCB, Quantico.

3. Confidential is the designation applied to information the unauthorized disclosure of which could reasonably be expected to cause damage to national security. Confidential OCAs at this Base will be the designated Top Secret and Secret OCAs indicated in previous paragraphs.

11002. CLASSIFICATION GUIDANCE. Inasmuch as it is impractical to attempt to cover all subjects dealing with classified information, MCCDC OCAs dealing with the following will consult chapter 4 of SECNAVINST 5510.36:

1. Original vs. derivative classification.
2. Original classification principles and considerations.
3. Specific classifying criteria.
4. Limitations on classifying.
5. Duration of original classification.
6. Challenges.
7. Resolution of conflicts.
8. Tentative classification.
9. Private information.
10. Foreign government information.

11003. OCA TRAINING. All OCAs shall be trained in the fundamentals of security classification, the limitations of their classification authority, and their OCA duties and responsibilities. This training is a prerequisite for an OCA to exercise this authority. OCAs shall provide written confirmation (i.e., indoctrination letter) to the Chief of Naval Operations (CNO) (N09N2) that this training has been accomplished. Training shall consist of a review of pertinent E.O.s, statutes, and DON regulations. The CNO (N09N2) will provide OCA training material upon request.

11004. DERIVATIVE CLASSIFICATION

1. While original classification is the initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, derivative classification is the incorporating, paraphrasing, restating, or generating, in new form, information that is already classified, and the marking of newly developed information consistent with the classification markings that apply to the classified source. This includes the classification of information based on duplication or reproduction of existing classified information. An estimated 99 percent of the classified information produced is derivatively classified.

2. Derivative classifier shall:

a. Observe and respect the original classification determinations made by OCAs (and as codified in classified source documents and security classification guides),

b. Use caution when paraphrasing or restating information extracted from a classified source document(s) to determine whether the classification may have been changed in the process,

c. Carry forward to any newly created information the pertinent classification markings.

11005. ACCOUNTABILITY OF CLASSIFIERS. Classifiers are accountable for the propriety of the classifications they assign, whether original or derivative. Those with Command signature authority must ensure that classification markings are accurate before they sign classified documents or approve classified material. Commanding officers may designate the organizational security manager as the approver of assigned derivative classifications.

11006. FOREIGN GOVERNMENT INFORMATION (FGI)

1. Information classified by a foreign government or international organization retains its original classification level or is assigned a U.S. classification equivalent (see exhibit 6c of SECNAVINST 5510.36) to that provided by the originator to ensure adequate protection of the information. Authority to assign the U.S. classification equivalent does not require original classification authority.

2. Foreign Government Unclassified and RESTRICTED information provided with the expectation, expressed or implied, that it, the source, or both are to be held in confidence shall be classified confidential. It may be classified at a higher level if it meets the damage criteria of paragraph 4-2 of SECNAVINST 5510.36.

11007. SYSTEMATIC REVIEWS

1. Information classified by the OCAs will be declassified as soon as national security considerations permit. Chapter 4 of SECNAVINST 5510.36 refers. Decisions concerning declassification or downgrading must be based on the loss of sensitivity of the information with the passage of time or the occurrence of an event that permits declassification or downgrading. Authority to downgrade or declassify should not be confused with the administrative responsibility of a holder of classified information to downgrade or declassify it as directed by a classification guide, continued protection guidelines, or the instructions on a document.

2. Although Navy and Marine Corps commands no longer require systematic reviews for declassification, MCB, Quantico activities will continue to conduct systematic reviews in the interest of reducing classified holdings to the lowest minimum necessary. This action will be monitored by the Command Security Manager (B 054) with emphasis on reducing vulnerability to security violations resulting from the accumulation of excessive amounts of classified material.

11008. CONTINUED PROTECTION GUIDELINES. Continued protection guidelines in OPNAVINST 5513.16A will be used in reviewing 25-year-old classified information held by MCB activities. DON information that is 25 years old and is not identified in the guidelines as requiring continued protection will be declassified.

11009. REQUESTS FOR MANDATORY DECLASSIFICATION REVIEW. Requests for mandatory declassification review are distinct from requests for records made under the Freedom of Information Act. Requests received for mandatory declassification review will be forwarded to the CG MCB (B 054) for action per chapter 4 of SECNAVINST 5510.36. Requests received for records made under the FOIA will be forwarded to the CG MCB (B 013).

11010. DECLASSIFICATION, DOWNGRADING, AND UPGRADING. A thorough review of chapter 4 of SECNAVINST 5510.36 should be made prior to the declassification, downgrading, and upgrading of classified material.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 12

SECURITY CLASSIFICATION GUIDES (SCGs)

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	12000	12-3
PREPARING SCGs	12001	12-3
RETRIEVAL AND ANALYSIS OF NAVY CLASSIFIED INFORMATION PROGRAM (RANKIN)	12002	12-3
PERIODIC REVIEW OF SCGs.	12003	12-4
CONFLICT BETWEEN A SOURCE DOCUMENT AND AN SCG	12004	12-4

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 12

SECURITY CLASSIFICATION GUIDES (SCGs)

12000. BASIC POLICY

1. Security Classification Guides (SCG) serve both legal and management functions by recording DON original classification determinations made under reference (a) and its predecessor orders. SCGs are the primary reference source for derivative classifiers to identify the level and duration of classification for specific information elements.

2. The DON original classification authority (OCA) listed in exhibit 4A of SECNAVINST 5510.36 are required to prepare a SCG for each DON system, plan, program, or project under their cognizance that creates classified information. Updates to exhibit 4A can be found on the Chief of Naval Operations (CNO) (NO9N2) Homepage at www.navysecurity.navy.mil. Security Classification Guides shall be issued as soon as practicable prior to initial funding or implementation of the relevant system, plan, program, or project. In support of this requirement, the CNO (NO9N2) manages a system called the Retrieval and Analysis of Navy Classified Information (RANKIN) Program, which manages and centrally issues SCGs for the DON OCAs.

12001. PREPARING SCGs. SCGs shall be prepared, in writing, in the format described in Executive Order 12958, and approved personally by an OCA who has both cognizance (i.e., program or supervisory responsibility) over the information, and who is authorized to originally classify information at the highest classification level prescribed in their SCG(s).

12002. RETRIEVAL AND ANALYSIS OF NAVY CLASSIFIED INFORMATION PROGRAM (RANKIN). The primary element of the RANKIN Program is a computerized database that provides for the standardization, centralized management, and issuance of all DON SCGs. After approval by an OCA, SCGs are forwarded to the CNO (NO9N2), RANKIN Program Manager, and entered into the RANKIN database. Additionally, the RANKIN Program Manager maintains historical files for all DON SCGs. Classification guides are detailed in chapter 5, paragraph 5-3 of OPNAVINST 5510.36.

12003. PERIODIC REVIEW OF SCGs. OCAs shall review their SCGs for accuracy and completeness at least every 5 years and advise the CNO (NO9N2) of the results. Proposed changes to, and cancellations of, existing SCGs shall be sent to the CNO (NO9N2) in the format described in OPNAVINST 5513.1E.

12004. CONFLICT BETWEEN A SOURCE DOCUMENT AND AN SCG. In case of apparent conflict between an SCG and a classified source document about a discrete item of information, the instructions in the SCG shall take precedence.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 13

MARKING

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	13000	13-3
BASIC MARKING REQUIREMENTS	13001	13-3
REPRODUCTION OF GUIDES	13002	13-3
FILES, FOLDERS, OR GROUPS OF DOCUMENTS	13003	13-3
TRANSMITTALS	13004	13-4
ELECTRONICALLY-TRANSMITTED MESSAGES	13005	13-4
CHARTS, MAPS, AND DRAWINGS	13006	13-4
REMOVABLE AUTOMATED INFORMATION SYSTEM (AIS) AND WORD PROCESSING STORAGE MEDIA	13007	13-4
DOCUMENTS PRODUCED BY AIS EQUIPMENT	13008	13-5
STANDARD DOWNGRADING/DECLASSIFICATION MARKINGS	13009	13-5
SECURITY DISCREPANCY NOTICE	13010	13-5
FIGURE		
13-1 SAMPLE SECURITY CONTAINER INFORMATION SF 700.		13-6
13-2 SAMPLE SECURITY DISCREPANCY NOTICE - OPNAV 5511/51		13-7

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 13

MARKING

13000. BASIC POLICY

1. The purpose of marking classified material is to inform the holder of the classification level, the degree of protection required, and to assist in extracting, paraphrasing, downgrading, and declassifying actions. All classified material must be marked in a manner that leaves no doubt about the level of classification assigned to the material, which parts contain or reveal classified information, how long the material must remain classified, and any additional measures necessary to protect the material.

2. Classified material will be physically marked, annotated, or identified as specified in chapter 6 of SECNAVINST 5510.36.

13001. BASIC MARKING REQUIREMENTS

1. Marking requirements and the application of markings vary, depending on the kind of material. For purposes of uniformity and to avoid redundancy, paragraph 13000 above is applicable.

2. Classification markings will be stamped, printed, or written in capital letters, larger than those used in the text document or conspicuously on other material, and, when practical, in the color red.

13002. REPRODUCTION OF GUIDES. The reproduction of guides utilizing Chapter 6 and exhibits 6A-1 through 6A-18 of SECNAVINST 5510.36 is encouraged for use by personnel responsible for proper marking of classified material.

13003. FILES, FOLDERS, OR GROUPS OF DOCUMENTS

1. When a file, folder, or group of classified documents is removed from secure storage, it must be conspicuously marked with the highest classification of any classified document it contains, with an appropriate classified document cover sheet attached.

2. The only document cover sheets authorized for use by activities at MCB, Quantico are as follows:

- a. Top Secret Cover Sheet, SF 703 - NSN 7540-01-213-7901.
- b. Secret Cover Sheet, SF 704 - NSN 7540-01-213-7902.
- c. Confidential Cover Sheet, SF 705 - NSN 7540-01-213-7903.

3. In addition, the following forms are to be used by all activities at this Base:

- a. Security Container Information Form, SF 700 - NSN 7540-01-214-5372 (figure 13-1).
- b. Activity Security Checklist, SF 701 - NSN 7540-01-213-7899 (figure 2-6).
- c. Security Container Check Sheet, SF 702 - NSN 7540-01-213-7900 (figure 2-7).

13004. TRANSMITTALS. When a transmittal document or endorsement is added to classified material, it must carry the highest classification of the information it transmits, and a statement showing the classification, if any, of the transmittal document standing alone. An unclassified letter, which transmits a classified document as an enclosure, would carry the classification of the enclosure and the notation, "unclassified upon removal of enclosure".

13005. ELECTRONICALLY-TRANSMITTED MESSAGES. Mark classified messages at the top and bottom with the overall classification and portion marked as prescribed for other documents. Due to black ink used in preparing messages, red ink is encouraged for marking classified messages.

13006. CHARTS, MAPS, AND DRAWINGS. Mark overall classification at the top and bottom of each document. Add additional markings that are clear when the document is rolled or folded.

13007. REMOVABLE AUTOMATED INFORMATION SYSTEM (AIS) AND WORD PROCESSING STORAGE MEDIA

1. External Markings. Removable information storage media and devices, used with AIS systems and typewriters or word processing

systems must be labeled using color-coded labels (Standard Forms 706, 707, 708, 709, 710, and 711 see page 6A-18 of SECNAVINST 5510.36) that indicate clearly the classification, and associated markings of the information they contain. Media and devices that store information recorded in the analog or digital form and are generally mounted or removed by the users or operators include magnetic tape reels, cartridges, cassettes, removable hard drives, CD ROM disks, disk cartridges, disk packs, diskettes, and magnetic cards.

2. Internal Markings. AIS and word processing systems will provide for internal markings to ensure that classified information, which is produced or generated, clearly shows the classification and associated markings. The Chief of Naval Operations (OP 09N) may exempt existing systems when internal marking requirements cannot be met without extensive system modification. Procedures must be established, however, to ensure that users and recipients of the media or information are clearly advised as to the classification and associated markings.

13008. DOCUMENTS PRODUCED BY AIS EQUIPMENT. These documents will be marked as prescribed in paragraph 6-34 of SECNAVINST 5510.36.

13009. STANDARD DOWNGRADING/DECLASSIFICATION MARKINGS. Mark this material per paragraph 6-10 of SECNAVINST 5510.36.

13010. SECURITY DISCREPANCY NOTICE. When classified material is received which is improperly or incompletely marked, or which does not show proper downgrading or declassification information, the Command Security Manager (B 054) will in turn notify the originator of the material by utilizing OPNAV Form 5511/51, Security Discrepancy Notice (figure 13-2).

INFORMATION AND PERSONNEL SECURITY PROGRAM

☆ U.S. GOVERNMENT PRINTING OFFICE: 1993—359-597

SECURITY CONTAINER INFORMATION				
INSTRUCTIONS				
1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP)				
2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER.				
3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER				
4. DETACH PART 2A AND INSERT IN ENVELOPE.				
5. SEE PRIVACY ACT STATEMENT ON REVERSE.				
10. Immediately notify one of the following persons, if this container is found open and unattended				
EMPLOYEE NAME	HOME ADDRESS	HOME PHONE		
1. ATTACH TO INSIDE OF CONTAINER				

700-101
NSN 7540-01-214-5372
STANDARD FORM 700 (8-85)
Prescribed by GSA/1500
32 CFR 2003

WARNING

WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.

DETACH HERE

CONTAINER NUMBER	
COMBINATION	
_____ Turns to the (Right) (Left) stop at _____	
_____ Turns to the (Right) (Left) stop at _____	
_____ Turns to the (Right) (Left) stop at _____	
_____ Turns to the (Right) (Left) stop at _____	
WARNING	
THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.	
UNCLASSIFIED UPON CHANGE OF COMBINATION	
2A	INSERT IN ENVELOPE
SF 700 (8-85) Prescribed by GSA/1500 32 CFR 2003	

Figure 13-1.--Sample Security Container Information SF 700.

INFORMATION AND PERSONNEL SECURITY PROGRAM

SECURITY DISCREPANCY NOTICE

OPNAV 5511/51 (5-80) S/N 0107-LF-055-5355 (This form replaces OPNAV 5511/8; 22 and 24 which are obsolete)

FROM	DATE
REF a. _____ (Insert ref. (a))	b. OPNAVINST 5510.1 SERIES
ENCL _____	

TO: {

(Note – This form may be mailed
in a window envelope.)

}

1. Reference (a) has been found to be inconsistent with or in contravention of reference (b) for the reason(s) checked below.
2. If applicable, corrective action should be taken and where this involves changing classification, all holders of reference (a) should be notified accordingly.

IMPROPER TRANSMITTAL/PACKAGING			
SENT VIA NON-REGISTERED/ NON-CERTIFIED MAIL		CLASSIFICATION NOT MARKED ON INNER CONTAINER	RECEIVED IN POOR CONDITION; COMPROMISE IMPROBABLE
SENT IN SINGLE CONTAINER		NO RETURN RECEIPT	ADDRESSED IMPROPERLY
MARKINGS ON OUTER CONTAINER DIVULGE CLASSIF. OF CONTENTS		INADEQUATE WRAPPING; NOT SECURELY WRAPPED OR PROTECTED	OTHER <i>(Specify)</i>
CLASSIFICATION			
BASIC CLASSIFICATION QUESTIONABLE		DOCUMENT SUBJECT MARKING	CHART, MAP OR DRAWING MARKING
OVERALL MARKINGS		DOCUMENT TRANSMITTAL MARKING	PHOTO, FILM OR RECORDING MARKING
PARAGRAPH/COMPONENT MARKINGS		MESSAGE MARKING	OTHER <i>(Specify)</i>
DOWNGRADING/DECLASSIFICATION			
CLASSIFICATION AUTHORITY NOT IDENTIFIED OR UNAUTHORIZED		DOWN GRADING DATA INCORRECT	DECLASSIFICATION (OR REVIEW) DATA OMITTED OR INCORRECT
OTHER <i>(Specify)</i>			

↑
Fold here with face of form in view

COMMENTS *(Continue on reverse, if necessary)*

COPY TO: OP-009D (WITH ADDRESSEE DELETED)

SIGNATURE	TITLE
-----------	-------

Figure 13-2.--Sample Security Discrepancy Notice OPNAV 5511/51.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 14

SAFEGUARDING

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	14000	14-3
RESPONSIBILITY	14001	14-3
RESTRICTED AREAS	14002	14-3
CONTROL MEASURES	14003	14-4
WORKING PAPERS	14004	14-5
SPECIAL TYPES OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION.	14005	14-6
ID CARDS AND BADGES	14006	14-6
CARE DURING WORKING HOURS	14007	14-7
END-OF-DAY SECURITY CHECKS	14008	14-7
SAFEGUARDING DURING VISITS	14009	14-8
SAFEGUARDING DURING CLASSIFIED MEETINGS. . .	14010	14-8
INVENTORY OF CLASSIFIED MATERIAL	14011	14-11
FIGURE		
14-1 SAMPLE TOP SECRET COVER SHEET		14-12
14-2 SAMPLE SECRET COVER SHEET		14-13
14-3 SAMPLE CONFIDENTIAL COVER SHEET . . .		14-14
14-4 SAMPLE CHANGE OF CUSTODIAN INVENTORY OF CLASSIFIED MATERIAL COVER LETTER .		14-15
14-5 SAMPLE SEMIANNUAL INVENTORY OF CLASSIFIED MATERIAL COVER LETTER. . .		14-16

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 14

SAFEGUARDING

14000. BASIC POLICY. Classified information or material will be used only where there are facilities or under conditions adequate to prevent unauthorized persons from gaining access to it. To the extent possible, classified holdings will be consolidated to limit the areas where it will be used. The exact nature of security requirements will depend on a thorough security evaluation of local conditions and circumstances provided by the CG MCB (B 054).

14001. RESPONSIBILITY

1. Anyone who has possession of classified material is responsible for safeguarding it at all times and particularly for locking classified material in an appropriate security container whenever it is not in use or under direct supervision of authorized persons. The custodian must follow procedures, which ensure that unauthorized persons do not gain access to classified information by sight, sound, or other means. Classified information will not be discussed with or in the presence of unauthorized persons.

2. Custodians will not remove classified material from a designated office or working area except in the performance of official duties and under conditions providing the protection required by SECNAVINST 5510.30A and SECNAVINST 5510.36. Under no circumstances will a custodian remove classified material from designated work areas to work on it during off duty hours, or for any other purpose involving personal convenience, without specific approval of the CG MCB (B 054).

14002. RESTRICTED AREAS

1. Do not designate controlled areas, limited areas, and exclusion areas in any way that outwardly note their relative sensitivity. Identify any such area as a "Restricted Area."

2. Personnel permitted after hour access to classified work or storage areas will be required to sign in and out on a log sheet, with the exception of facilities operated 24/7.

14003. CONTROL MEASURES

1. All top secret information (including copies) originated or received by a command shall be continuously accounted for, individually serialized, and entered into a command top secret log. The Top Secret Control Officer (TSCO) for MCB, Quantico is located at Security Branch, Classified Material Control Center (CMCC) and is the primary custodian for all Top Secret material held at MCB, Quantico.

2. The Base CMCC is a decentralized facility, therefore, with the exception of special category classified and Top Secret material, Secret documents will not be retained at the CMCC but at the division level Secondary Control Point (SCP).

a. Secret material originated locally or received by other commands will be entered into the Automated Security Control Program (ASCP). This includes all material coming in through official mail addressed to an activity or individual and material hand carried by personnel of this or other commands and organizations.

b. All secret documents leaving the CMCC to the SCP's will have with them two classified material control forms that identify the document. One copy of the control form is to be signed and dated by the SCP, and retained as a receipt by the CMCC until that document appears on the next reported inventory. The second control form is for use by the SCP's for their local accountability requirements. Document control forms are unclassified and may be reproduced locally.

c. The destruction of documents under ASCP control will be accomplished per chapter 17 of this manual and SECNAVINST 5510.36.

3. Commanding officers shall establish administrative procedures for the internal control of Secret and Confidential information (*including items controlled by the ASCP*) appropriate to their local environment, based on an assessment of the threat, location, and mission of their command. These procedures shall be used to protect secret and confidential information from unauthorized disclosure by access control and compliance with the marking, storage, transmission, and destruction requirements of this manual and SECNAVINST 5510.36.

14004. WORKING PAPERS

1. Working papers include classified notes from training courses or conferences, research notes, drafts, and similar items that are not finished documents. Working papers that contain classified information shall be:

- a. Dated when created;
- b. Conspicuously marked "Working Papers" on the first page in letters larger than the text;
- c. Marked centered top and bottom on each page with the highest overall classification level of any information they contain;
- d. Protected per the assigned classification level; and
- e. Destroyed by authorized means when no longer needed.

2. Commanding officers shall establish procedures to account for, control, and mark all working papers in the manner prescribed for a finished document of the same security classification level when retained more than 180 days from date of creation or officially released outside the organization by the originator.

3. Secret Internet Protocol Router Network (SIPRNET) e-mail and their attachments will not automatically be identified and marked as Working Papers.

a. Classification marking of SIPRNET email and attachments will be per chapter 13 of this manual and chapter 6 of SECNAVINST 5510.36. Unlike Unclassified but Sensitive Internet Protocol Router Network (NIPERNET) e-mail, which is always unclassified, unclassified SIPRNET e-mail must be plainly marked as "unclassified" prior to sending, printing or downloading.

b. When SIPRNET e-mail is classified secret or confidential, then the highest classification will be properly marked and all portion markings completed prior to sending, printing, or downloading (chapter 13 of MCBO 5510.1B).

c. If clarification is required on the overall classification of SIPRNET email and especially on any missing portion markings, then the originator is the only authority that can clearly identify and mark/re-mark any questionable information.

d. As well as classification and portion marking, the originating source of classified information must also be identified along with its appropriate declassification instructions (chapters 11 and 12 of MCBO 5510.1B).

e. Further, all documentation identified in this category **not** conforming to the regulations provided will be considered a violation of security practices and will not be looked on favorably during inspections.

14005. SPECIAL TYPES OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION. Control and safeguard special types of classified information as follows:

1. Naval Warfare Publications (NWP). NWP 1-01 requires an administrative system for controlling the NWP Library within the command. Classified NWPs shall be safeguarded per SECNAVINST 5510.36, according to their security classification level. Administrative controls for NWPs do not replace the security controls required for classified information.

2. North Atlantic Treaty Organization (NATO). NATO classified documents will not be intermingled with U.S. documents in storage containers. NATO documents may be filed in the same drawer of a security container with U.S. documents if they are segregated and clearly identified as NATO files. Control and safeguard NATO classified information (including NATO Restricted) per OPNAVINST 5510.101D.

3. Control and protect all other special category information (e.g., FGI, RD, CNWDI, FRD, COMSEC, SAP'S NNPI, SBU, DEASI, and DoD UCNI) per chapter 7, paragraph 7-7 of SECNAVINST 5510.36.

14006. ID CARDS AND BADGES. Activities using an ID/badge systems will comply with the provisions of OPNAVINST 5530.14C, bearing in mind that classified information will not be disclosed or released solely on the basis of a card or badge. The MCB access roster and the Command Security Manager are available for assistance in this matter.

14007. CARE DURING WORKING HOURS

1. Keep classified information under constant surveillance by an authorized person at all times. When classified documents are removed from storage for working purposes, keep them face down or covered when not in use with classified material cover sheets, Standard Forms 703, 704, and 705, will be used. (figures 14-1, 14-2, and 14-3)
2. Discuss classified information only when unauthorized persons cannot overhear the discussion. Take particular care when there are visitors or maintenance personnel present. Escorts should alert fellow workers when visitors or workmen are in the area. Practice the need-to-know principle.
3. Protect preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, and all similar items containing classified information. Further protect this material by taking it to secondary control points for proper destruction immediately after they have served their purpose, or by giving them the same classification and safeguarding them in the same manner as the classified material they provided.
4. Protect computer printer and typewriter ribbons, computer storage media, and other classified items according to their security classification level.
5. In a mixed working environment (i.e., classified and unclassified), automated information system media used for processing or storing classified information shall be marked with an SF 706, 707, 708, 709, 710, 711, or 712 Sensitive Compartmented Information, as applicable. In a totally unclassified working environment, SF labels are not required.

14008. END-OF-DAY SECURITY CHECKS

1. Commanding officers and activity heads will require a security check at the end of each working day to make sure all classified material is properly secured.
2. Sample procedures for activity security checks are in figure 2-7. Those conducting security checks will make sure that:

a. Security containers have been locked. The Security Container Check Sheet, SF 702 (figure 2-8) will be used as the opening and locking record for all security containers, vaults and secure rooms. Appropriate entry's will be made on SF 702 each time a container or vault/secure room is opened and locked, but need only be double checked after the last locking for that day.

b. The contents of desks, wastebaskets and other surfaces and receptacles containing classified material have been properly stored or destroyed.

c. Windows and doors have been locked.

d. All classified material is stored in the manner prescribed and that burn bags are properly stored or destroyed.

e. Security alarms(s) and equipment have been activated.

f. Check other items as directed (i.e. STU III phones, power off on shredders, computers, copiers etc.).

3. All SF 702 forms used to record the opening and locking of security containers, vaults/secure rooms that contain COMSEC information/material will be retained for 2 years. The SF 701 form and all other SF 702 forms will be maintained for 30 days (current month plus previous month).

14009. SAFEGUARDING DURING VISITS. Commanding officers shall establish procedures to ensure that only visitors with an appropriate clearance level and need-to-know are granted access to classified information. At a minimum, these procedures shall include verification of the identity, clearance level access (if appropriate), and need-to-know for all visitors. Refer to SECNAVINST 5510.30A for visit procedures.

14010. SAFEGUARDING DURING CLASSIFIED MEETINGS

1. Classified information will not be disclosed at conferences, symposia, exhibits, conventions, seminars, or other gatherings (hereafter called meetings) unless disclosure of the information serves a government purpose and adequate security measures are taken to control access to the information and prevent its compromise.

2. A meeting conducted or sponsored by any activity at this Base in which classified information will be disclosed must be held at a cleared facility and only after determining that:

a. Disclosure of classified information at a meeting is in the best interest of national security.

b. The use of conventional channels for dissemination of classified information will not accomplish the purpose of the meeting.

c. The location selected facilitates proper control and dissemination of classified information including secure storage.

d. Adequate security measures and access procedures will be imposed.

e. Attendance will be limited strictly to those persons whose presence is considered necessary in the interests of national security.

f. All persons to be invited who are not cleared members of the Executive Branch of the government or cleared DoD contractor employees have been identified so Limited Access Authorizations or Foreign Disclosure Authorizations may be processed.

3. The center, Base, or activity head sponsoring a meeting at which classified information is to be disclosed is responsible for ensuring that visit requests for attendees are on file prior to conducting the meeting. The center, Base, or activity point of contact will coordinate with the Command Security Manager to verify classified material access eligibility of attendees.

4. Marine Corps and Navy personnel at this Base must have the approval of their division directors/commanding officers to disclose classified information at meetings conducted by or under security sponsorship of other bases or agencies of the Executive Branch of the government.

5. Marine Corps or Navy commands conducting or providing security sponsorship for classified meetings must ensure that:

a. Areas in which classified information is to be discussed afford adequate security against unauthorized access.

b. Adequate storage facilities are available.

c. Each person attending has been authorized access to information of equal or higher classification than the information being disclosed.

d. Admittance is limited to those on an approved access list and then only upon proper identification. Strict compliance with this requirement is especially critical when a classified meeting has been announced publicly.

6. Each person who is to disclose classified information must be notified of the security limitations that must be imposed because of:

a. The level of access authorized for all attendees.

b. "Need-to-know" of attendees.

c. Physical security conditions.

d. Provisions have been made to control and safeguard classified material given to those attending and to retrieve the material or effect transfer of control through approved methods.

e. Sessions are monitored to ensure discussions are limited to the level authorized.

f. Classified notes received or taken will be controlled per paragraph 14004 of this manual.

7. A person who is neither a cleared member of the Executive Branch of the government nor a cleared DoD contractor employee cannot attend a classified meeting sponsored by a Navy or Marine Corps command without approval by the Chief of Naval Operations (OP 09N). Authorization must be obtained before issuing an invitation.

8. All study groups being formed aboard this Base, to include HQMC activities, will coordinate with the CG MCB (B 054) prior to utilizing classified material. A 30-day period is required for security planning purposes.

9. Compromising emanations inspections and technical surveillance countermeasures inspections are mandatory for study groups utilizing Top Secret material, and when Secret material is discussed on a continuous basis within the study group area.

10. Individuals assigned to any study group who will utilize any classified material will be placed on the MCB Classified Material Access List. The granting of interim Top Secret clearances to gain access to Top Secret material is discouraged.

11. All MCB orders and other applicable security directives will be followed by study groups.

12. When it becomes necessary to provide temporary storage of classified material brought aboard MCB, Quantico after normal working hours, the CMCC duty clerk will be notified by phone or pager, and the CMCC will act as the overnight repository for classified material (up to secret level) hand-carried by visitors from other commands. This measure is an emergency measure to protect classified material when prior arrangements for storage of classified material cannot be made. Personnel from the CMCC will secure the material in the CMCC located at 3300 Russell Road, room 310 until called for by appropriate authority.

14011 INVENTORY OF CLASSIFIED MATERIAL

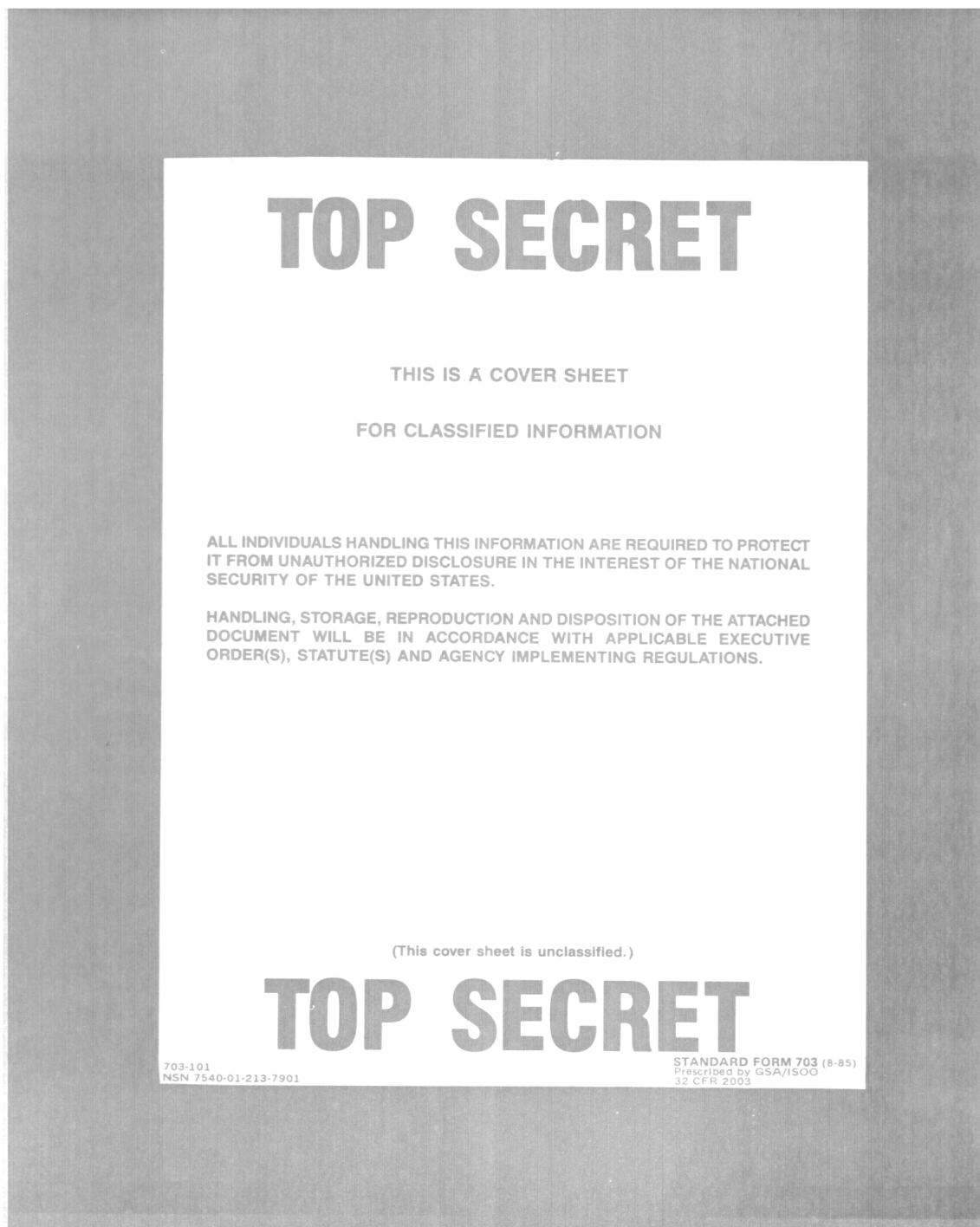
1. A change of custodian inventory must be conducted and submitted to the Head, Document Control Section, CMCC, upon relief of a SCP custodian. The incoming custodian must complete and sign the inventory prior to the departure of the outgoing custodian and the assumption of the account. The SCP Security Manager verifies the inventory, figure 14-4.

2. A local computer-generated inventory printed from the Automated Security Control Program (ASCP) will be conducted semiannually (the last working day of January and July) for verification by the SCP Security Manager. Once the material has been physically sighted, the verified inventory will be submitted to the Head, Document Control Section, CMCC, within 10 working days, figure 14-5.

3. An unannounced inspection inventory of all accountable secret controlled material on retention within an activity will be conducted annually by personnel from the CMCC, the inventory will be a physical sighting and examination of written evidence of proper accountability, destruction, transfer, etc. During inventories, documents will be audited to determine completeness, accuracy of markings, serial numbers (bar codes), declassification/downgrading instructions, and related control dates.

4. All inventories conducted by personnel from the CMCC, are based on the holdings listed in the Master Data Base of the ASCP.

INFORMATION AND PERSONNEL SECURITY PROGRAM

A sample Top Secret Cover Sheet, which is a white rectangular document centered on a dark gray background. The document features the words "TOP SECRET" in large, bold, black capital letters at the top and bottom. Between these, the text "THIS IS A COVER SHEET" and "FOR CLASSIFIED INFORMATION" is centered. Two paragraphs of smaller text provide instructions on handling the information. A note in parentheses states "(This cover sheet is unclassified.)". At the bottom left, it says "703-101 NSN 7540-01-213-7901". At the bottom right, it says "STANDARD FORM 703 (8-85) Prescribed by GSA/ISOO 32 CFR 2003".

TOP SECRET

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT WILL BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

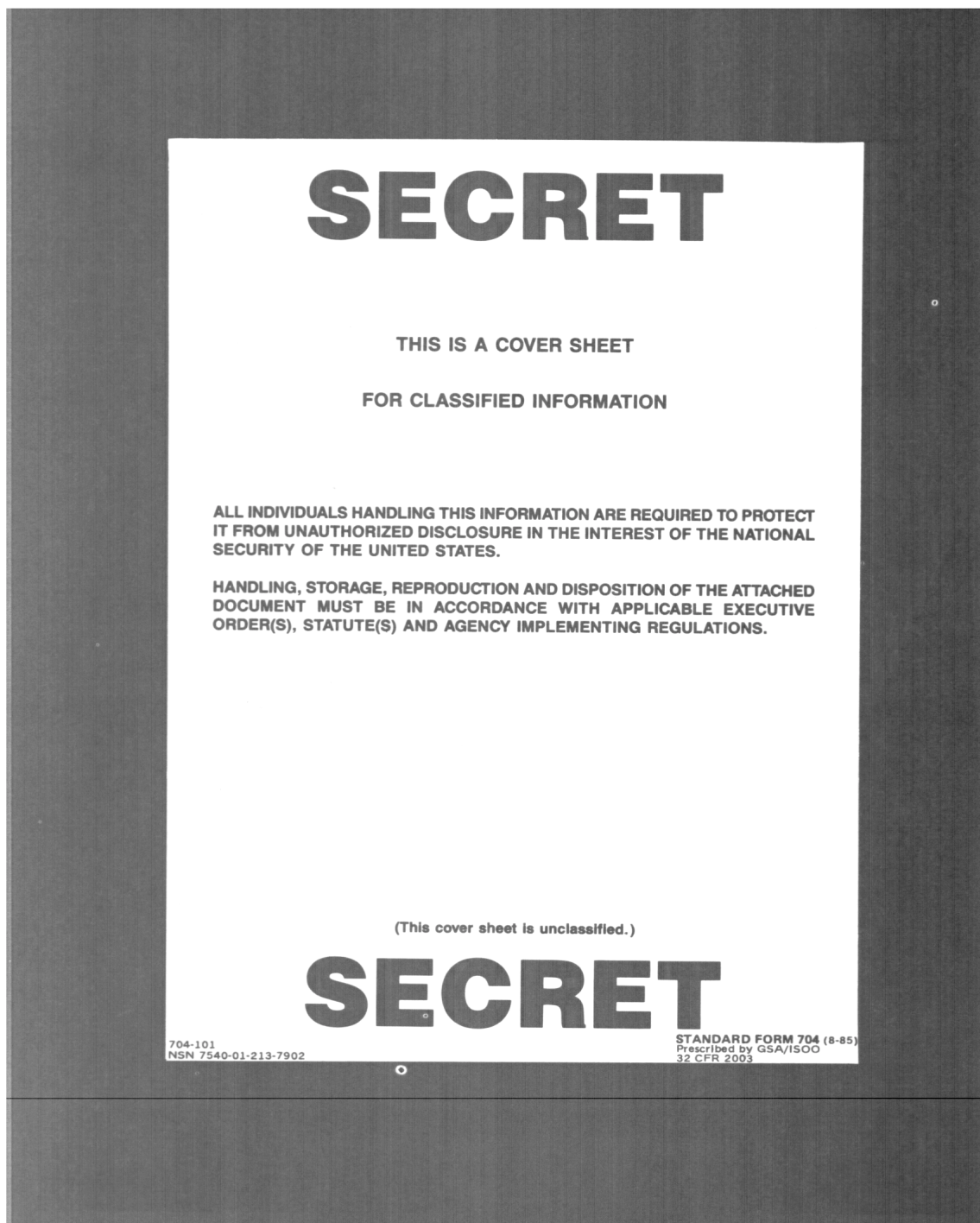
TOP SECRET

703-101
NSN 7540-01-213-7901

STANDARD FORM 703 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

COLOR ORANGE

Figure 14-1.--Sample Top Secret Cover Sheet.

A sample of a Secret Cover Sheet, which is a white rectangular document centered on a dark gray background. The word "SECRET" is printed in large, bold, black capital letters at the top and bottom. Between the top and bottom "SECRET" words, the text "THIS IS A COVER SHEET" and "FOR CLASSIFIED INFORMATION" is centered. Below this, two paragraphs of text are centered: "ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES." and "HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS." Below the second paragraph, the text "(This cover sheet is unclassified.)" is centered. At the bottom left, the text "704-101" and "NSN 7540-01-213-7902" is printed. At the bottom right, the text "STANDARD FORM 704 (8-85)" and "Prescribed by GSA/ISOO 32 CFR 2003" is printed.

SECRET

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

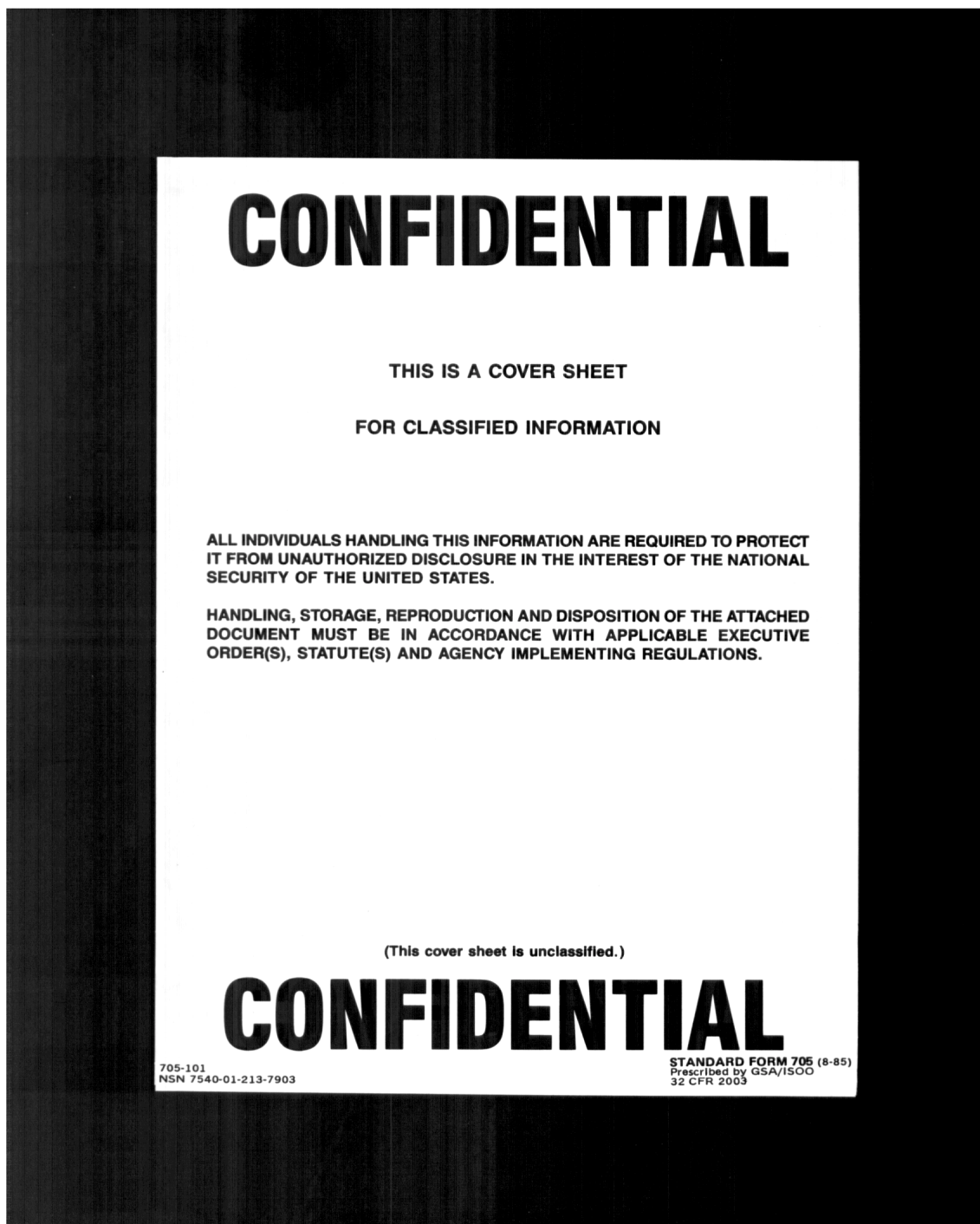
SECRET

704-101
NSN 7540-01-213-7902

STANDARD FORM 704 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

COLOR RED

Figure 14-2.--Sample Secret Cover Sheet.

A sample of a Confidential Cover Sheet, Standard Form 705. The sheet is white with black text, set against a dark background. At the top, the word "CONFIDENTIAL" is printed in large, bold, sans-serif capital letters. Below this, the text "THIS IS A COVER SHEET" and "FOR CLASSIFIED INFORMATION" are centered. A paragraph states: "ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES." Another paragraph states: "HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS." Below these, a note in parentheses says "(This cover sheet is unclassified.)". At the bottom, the word "CONFIDENTIAL" is printed again in large, bold, sans-serif capital letters. In the bottom left corner, the text "705-101" and "NSN 7540-01-213-7903" is printed. In the bottom right corner, the text "STANDARD FORM 705 (8-85)", "Prescribed by GSA/ISOO", and "32 CFR 2003" is printed.

COLOR BLUE

Figure 14-3.--Sample Confidential Cover Sheet.

INFORMATION AND PERSONNEL SECURITY PROGRAM

LETTER HEAD

5510
(Originator Code)
(Date)

From: Activity/Secondary Control Point
To: Commanding General, Marine Corps Base (B 054) (Attn:
Head, Document Control Section, CMCC)

Subj: CHANGE OF CUSTODIAN INVENTORY OF CLASSIFIED MATERIAL

Ref: MCBO 5510.1B

Encl: ASCP, print out of inventoried material

1. Per the reference, a change of custodian inventory of all controlled SECRET holdings was conducted on (DATE). The enclosure is a detailed list of classified material, held by this sub-account.

2. Point of Contact for this matter is (Primary Custodian or Alternate or Security Coordinator), (telephone number).

(Incoming Custodian)
SIGNATURE

(Security Manager)
SIGNATURE
Verified by

Copy to:
CG MCB (B 054)
Unit/Acty Scty Mgr

Figure 14-4.--Sample Change of Custodian Inventory of Classified Material Cover Letter.

INFORMATION AND PERSONNEL SECURITY PROGRAM

LETTER HEAD

5510
(Originator Code)
(Date)

From: Activity/Secondary Control Point
To: Commanding General, Marine Corps Base (B 054) (Attn:
Head Document Control Section, CMCC)

Subj: SEMIANNUAL INVENTORY OF CLASSIFIED MATERIAL

Ref: MCBO 5510.1B

Encl: ASCP, print out of inventoried material

1. Per the reference, a semiannual inventory of all controlled SECRET holdings was conducted on (DATE). The enclosure is a detailed list of classified material, held by this sub-account.

2. Point of Contact for this matter is (Primary Custodian or Alternate or Security Coordinator), (telephone number).

(Incoming Custodian)
SIGNATURE

(Security Manager)
SIGNATURE
Verified by

Copy to:
CG MCB (B 054)
Unit/Acty Scty Mgr

Figure 14-5.--Sample Semiannual Inventory Of Classified Material
Cover Letter.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 15

DISSEMINATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	15000	15-3
DISSEMINATION THROUGH JUDICIAL PROCEDURES	15001	15-3
DISSEMINATION TO DoD CONTRACTORS	15002	15-3
DISCLOSURE TO FOREIGN GOVERNMENTS, INTERNATIONAL ORGANIZATIONS, AND CONGRESS. .	15003	15-4
DISSEMINATION OF INTELLIGENCE	15004	15-4

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 15

DISSEMINATION

15000. BASIC POLICY

1. Dissemination of classified material will be limited to those activities having a need-to-know and will reflect all applicable restrictions imposed by the originator and higher authority.
2. Material prepared for public release will not contain classified material or prescribed technical data. Policies and procedures governing public release of official information and the circumstances under which a security review is required are detailed in SECNAVINST 5720.44 and MCO 5510.9B and will be coordinated through the Public Affairs Office.
3. For information and appropriate references pertaining to Special Access Programs, material originating in a non-DoD department or agency, restricted and formerly restricted data, North Atlantic Treaty Organization material, cryptographic information, and Single Integrated Operational Plan information, refer to chapter 9 of SECNAVINST 5510.30A and chapter 8 of SECNAVINST 5510.36.
4. Distribution of all controlled unclassified information will be per chapter 8, paragraph 8-4 of SECNAVINST 5510.36.

15001. DISSEMINATION THROUGH JUDICIAL PROCEDURES

1. Convening authorities through judicial proceedings will make every effort to declassify that classified material which will be introduced as evidence.
2. If classified information is required for prosecution during a trial, the officer exercising general court-martial jurisdiction will notify the Command Security Manager (B 054) so that appropriate personnel security clearances can be granted per chapter 9 of SECNAVINST 5510.30A.

15002. DISSEMINATION TO DoD CONTRACTORS. Before disclosing any classified information to a DoD contractor, releasing activities or contractor commands must determine that the contractor has a current facility security clearance equal to or higher than the level of classified information to be disclosed. This may be done using visit request information and information provided by the Command Security Manager (B 054).

15003. DISCLOSURE TO FOREIGN GOVERNMENTS, INTERNATIONAL ORGANIZATIONS, AND CONGRESS. Authority for disclosure of classified information to foreign governments has been centralized in the Navy International Program Office. Accordingly, the disclosure of classified information by oral, visual, or written communications, or by any other means, to foreign governments or international organizations must be authorized in writing. Requests and approvals/disapprovals will be processed via the Command Security Manager (B 054).

15004. DISSEMINATION OF INTELLIGENCE. Prior to foreign dissemination of classified information or release of intelligence to contractors, chapter 8 of SECNAVINST 5510.36 and other applicable directives will be reviewed and the Command Security Manager (B 054) notified.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 16

TRANSMISSION AND TRANSPORTATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	16000	16-3
TOP SECRET	16001	16-3
SECRET	16002	16-3
CONFIDENTIAL	16003	16-3
TELEPHONE TRANSMISSION	16004	16-3
RECEIPT SYSTEM	16005	16-4
TRANSMISSION OF CLASSIFIED MATERIAL TO FOREIGN GOVERNMENTS	16006	16-4
TRANSMISSION OF COMMUNICATIONS SECURITY MATERIAL	16007	16-4
PREPARATION OF CLASSIFIED MATERIAL FOR TRANSMISSION	16008	16-4
ADDRESSING	16009	16-5
GUARD MAIL	16010	16-6
ELECTRICAL TRANSMISSION	16011	16-6
HANDCARRYING WITHIN A COMMAND OR IMMEDIATE ENVIRONS	16012	16-6
ADDITIONAL GUIDANCE	16013	16-8

FIGURE

16-1	SAMPLE - CLASSIFIED MATERIAL CONTROL FORM.	16-9
16-2	COURIER ADVISORY	16-10

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 16

TRANSMISSION AND TRANSPORTATION

16000. BASIC POLICY. Classified information will be transmitted in the custody of an appropriately cleared individual or by an approved system or carrier per the provisions of chapter 9 of SECNAVINST 5510.36.

16001. TOP SECRET. Top Secret material is received via the Defense Courier Service (DCS). The Base Top Secret Control Officer (TSCO) and the designated assistant located at the Classified Material Control Center (CMCC) are the official Top Secret couriers for this Base.

16002. SECRET. Secret material will normally be transmitted via the U.S. Postal Service (USPS) registered mail within and between the U.S. and its territories subject to the guidelines contained in Chapter 9 of SECNAVINST 5510.36. For overnight service, USPS Express Mail is permitted with prior approval from the Base Adjutant. Federal Express can be used to transmit secret and confidential material and shall only be used when it is the most cost-effective method of transmission given the constraints of time, security, and accountability. Federal Express and USPS registered mail can be shipped on Mondays through Thursdays to ensure that it is not stored at unsecured facilities over a weekend.

16003. CONFIDENTIAL. Confidential material will normally be transmitted by Registered, First Class, or Certified mail per the guidelines contained in SECNAVINST 5510.36.

16004. TELEPHONE TRANSMISSION. Classified information will not be transmitted over the telephone except as may be authorized on approved secure communication circuits. The practice of stating "This is not a secure line" is not a DON requirement. DD Form 2056 decals will be placed on all official Base telephones to alert users not to discuss classified information and that the telephones are subject to monitoring at all times. Unless special equipment is being used, there is no reason to believe a line is secure. Therefore, any discussion of classified information or "talking around" classified material is prohibited and unnecessary with the availability of STU/STE telephones.

16005. RECEIPT SYSTEM

1. Transmit top secret material under a continuous chain of receipts.
2. Secret material will be controlled by a signed receipt between commands and other authorized addresses. Failure to sign and return a receipt to the sender may result in a report of a possible compromise. Receipts are in the form of electronic signature via Automated Security Control Program (ASCP), hard copy of a Classified Material Control Form, ASCP (figure 16-1), or OPNAV Form 5511/10.
3. Local receipts for confidential materials are not required.
4. Classified material to be sent from this Base or its tenant activities will be turned in to the CMCC for processing and forwarding. The CMCC is responsible for all receipts and transmittals that will accompany the information. The receipt form will be unclassified and contain only the information necessary to identify the material being transmitted.

16006. TRANSMISSION OF CLASSIFIED MATERIAL TO FOREIGN GOVERNMENTS.
Refer to chapter 9 of SECNAVINST 5510.36 exhibit 9A.

16007. TRANSMISSION OF COMMUNICATIONS SECURITY MATERIAL.
Communication Security Material will be transmitted per CMS-21A (NOTAL). Consult the Commands Staff CMS Responsibility Officer (SCMSRO) and Electronic Key Management System (EKMS) Manager prior to transmission of this material.

16008. PREPARATION OF CLASSIFIED MATERIAL FOR TRANSMISSION

1. When classified material is transmitted, enclose it in two opaque, sealed envelopes or similar wrappings, where size permits, except as provided in paragraph 16008.2 below.
 - a. Fold or pack classified written material so the text will not be in direct contact with the inner envelope or container.
 - b. Show, on the inner envelope or container, the address of the receiving activity, highest classification of the material enclosed including, where appropriate, the "Restricted Data" marking and any special instructions. Seal it carefully to minimize the possibility of access without leaving evidence of tampering. Attach the receipt required for top secret and secret material.

c. Do not put on the outer cover a classification marking, a listing of the contents divulging classified information, or any other unusual data or marks which might invite special attention to the fact that the contents are classified.

2. Whenever the classified material being transmitted is too large to prepare as in paragraph 16008.1 above, wrap item in two opaque sealed containers, such as boxes or heavy wrappings. If the classified material is an internal component of a packaged item of equipment, the outside shell or body may be considered as the inner enclosure, which means that the packaged item of equipment need only be wrapped once.

16009. ADDRESSING

1. Address classified material to an official government activity or DoD contractor and **not to an individual**. This requirement is not intended, however, to prevent use of office code numbers or such phrases in the address as "Attention: Mr. Robert Allen," or similar aids in expediting internal routing, in addition to the organization address.

2. Consult the following publications for complete and correct mailing addresses and mailing instructions:

a. Standard Navy Distribution List, Part 1. contains the official list of fleet and mobile units and their administrative addresses.

b. Catalog of Naval Shore Activities, including Standard Navy Distribution List, Part 2. contains the official list of shore activities with complete administrative addresses.

3. The inner envelope or container will show the address of the receiving activity, the address of the sender, the highest classification level of the contents, including all warning notices. (See chapter 6, paragraphs 6-11 and 6-12 of SECNAVINST 5510.36.)

4. An outer envelope or container will show the complete and correct address of the recipient and the return address of the sender.

5. Care must be taken to ensure that classified material intended only for the U.S. elements of international staffs or other organizations are addressed specifically to those elements and that the correct address for classified mail is used for overseas locations. At **NO** time will classified information of any type be mailed to a post office box.

16010. GUARD MAIL. The use of guard mail to transmit classified material of any kind is **strictly prohibited**, and will result in a preliminary investigation (PI). See chapter 12 of SECNAVINST 5510.36.

16011. ELECTRONIC TRANSMISSION. Transmission of classified material by standard Naval telecommunications or the Defense Message System (DMS) is under the cognizance of the AC/S, G-6 MCB.

16012. HANDCARRYING WITHIN A COMMAND OR IMMEDIATE ENVIRONS

1. Only the Command Security Manager (B 054) will issue courier authorizations. Every precaution must be taken to prevent unauthorized disclosure when individuals are handcarrying classified material within this Base in the pursuit of daily duties or outside this Base in an official travel status.

2. When classified material is being carried within this Base or its immediate environs as part of normal duties, reasonable precautions will be taken to prevent inadvertent disclosure. Reasonable precautions include using an envelope, file folder, or whatever covering is needed to protect against casual observation of classified information. The precautions are to be taken when the movement is from one building to another, in an elevator, or through public areas.

3. If the movement requires transportation other than walking, double wrap the classified material. A locked briefcase may be considered the outer wrapping, except when hand carrying aboard commercial aircraft.

4. Because of the security risk inherent in handcarrying classified material while in a travel status, off base authorization will only be given when:

a. The classified material is required at the traveler's destination.

b. The classified material is not available at the visited destination.

c. Because of time or other constraints, the classified material cannot be transmitted by another authorized means.

5. Requests to handcarry classified material aboard U.S. flag carrying commercial aircraft may be originated with department heads. Requests will then be forwarded to the Command Security Manager via the activity heads (designated security managers), and will contain the following:

a. Full name of the individual and their employing agency or command.

b. Military/civilian picture identification card (DD Form 2) and (DD Form 2/OF55).

c. Dates classified material is to be carried, not to exceed 7 days.

d. Description of material to be carried (e.g., 3 sealed packages, 9" x 8" x 24"), address, and sender.

e. Itinerary of travel, listing points of departure, destinations, and known transfer points.

f. Level of classified material to be transported.

g. Destination point of contact (full name, address, and telephone number).

6. Upon receipt of the request containing all information listed above and the information to be transported, a courier letter authorization will be completed. The designated courier will then personally receipt for the authorization at the MCB Security Manager's Office, Bldg. 3300, and receive the briefing as required by SECNAVINST 5510.36.

7. A Universal Courier Authorization Card, DD Form 2501, has been developed, and supersedes all other command developed courier authorizations except for the NAVINTCOM 5510-69 (Rev 9-86), Sensitive Compartmented Information Courier Card. Use of DD Form 2501 is mandatory and exceptions or waivers from their use will not be granted. DD Form 2501 is authorization for local CONUS and outside

CONUS handcarry of classified material only and does not constitute authority for handcarrying classified material on commercial aircraft. In addition to DD Form 2501, a courier letter is necessary for handcarrying classified information on commercial aircraft. The expiration date of DD Form 2501 will not exceed 36 months from issue date.

a. The Command Security Manager is responsible for the procurement, accountability, and issuance of all DD Form 2501 cards for this Base and its tenant activities, except for HMX-1. HMX-1 will be responsible for both DD Form 2501 cards and letter courier authorizations involving HMX-1 personnel.

b. Activity security managers are responsible for ensuring accountability of all classified material given to couriers (including working papers). Activity security managers are also responsible for obtaining a signed briefing form for retention upon issuing classified material for handcarrying off station.

c. Couriers are responsible for signing a briefing form acknowledging an understanding of the regulations governing the handcarrying of classified material (figure 16-2). They are also responsible for providing their activity security managers with inventories of classified material being handcarried from the confines of this Base to another destination prior to departure.

16013. ADDITIONAL GUIDANCE. For additional information pertaining to aircraft and the conduct of passengers, refer to chapter 9 of SECNAVINST 5510.36.

INFORMATION AND PERSONNEL SECURITY PROGRAM

Classified Material Control Form The Attached Material is Classified				
<u>Command Control Number</u>			<u>ORIGINATOR</u>	
Received From: Document Date: Total Pages: Copy Number:			ENCLOSURES	
Subject: Short Title Long Title				
<u>Document Routing</u>				
Route to Directorate:			Intermediate Level Identification:	
NAME	Action	Date	Signature	Returned
<u>Declassification Information</u>				
Reason for Classification or Exemption Catagory:			Declassification Date:	
Remarks:				
REGISTERED #/COURIER #			<u>Command Control Number</u>	
Date Printed: 6/17/99			<u>The Attached Material is Classified:</u>	

Figure 16-1.--Classified Material Control Form.

INFORMATION AND PERSONNEL SECURITY PROGRAM

COURIER ADVISORY

Person Assigned Courier Duty _____
Last Name First Name M.I.

Card Number _____

Special Instructions:

1. I have reviewed and understand the provisions of chapter 16 of MCBO 5510.1B (Information and Personnel Security Program) and chapter 9 of SECNAVINST 5510.36 (Information Security Program Regulation).
2. I understand that classified materials will be placed in unmarked, double-sealed envelopes and will be in my physical possession at all times. The outer envelope will contain the address of the command where the information originated and the name of an official to contact in the event of an emergency. The inner envelope will be marked with the highest classification of classified material contained within.
3. An inventory of the document(s) to be transported and/or received from another agency or activity will be given to the respective security representative of the unit, activity, or organization with a copy forwarded to the Command Security Manager (B 054).
4. The classified material must be in my physical possession at all times, unless proper storage at a U.S. Government activity or appropriately cleared contractor facility (continental U.S. only) is available. Hand-carrying classified material on trips that involve an overnight stopover is not permitted without advance arrangements for proper overnight storage in a government activity or a cleared facility. When I surrender any package containing classified material for temporary storage (e.g., overnight or during meals), I must obtain a receipt signed by an authorized representative of the contractor facility or government installation accepting responsibility for safeguarding the package.

Figure 16-2.--Courier Advisory.

INFORMATION AND PERSONNEL SECURITY PROGRAM

COURIER ADVISORY

5. I may not read, study, display, or use classified material in any manner on a public conveyance or in a public place.

6. When the classified material is carried in a private, public, or government conveyance, I will not store it in any detachable storage compartment such as an automobile luggage rack, aircraft travel pod, or drop tank.

7. A list of all classified material carried or escorted by me will be maintained by my command. Upon my return, I must account for all classified material.

8. I will not remove classified information or material from officially designated offices or working areas for the purpose of working on such materials during off-duty hours.

9. I hereby certify that I have been briefed on the special requirements of courier duty and have been given a copy of this advisory containing special instructions for courier authorization.

Individual's Signature Date

Figure 16-2.--Courier Advisory Continued.

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 17

STORAGE AND DESTRUCTION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	17000	17-3
STORAGE REQUIREMENTS	17001	17-3
COMBINATIONS, LOCKS, AND KEYS	17002	17-4
PROCUREMENT AND TURN-IN OF SECURITY CONTAINERS	17003	17-5
DESTRUCTION OF CLASSIFIED INFORMATION. . .	17004	17-5
DESTRUCTION METHODS AND STANDARDS.	17005	17-6
DESTRUCTION PROCEDURES	17006	17-7
DESTRUCTION OF UNCLASSIFIED MATERIAL . . .	17007	17-8
FIGURE		
17-1 SAMPLE SECURITY CONTAINER RECORDS FORM		17-10

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 17

STORAGE AND DESTRUCTION

17000. BASIC POLICY

1. Commanding officers, directors, and activity heads are responsible for safeguarding all classified information within their organizations. They must ensure that it is stored as prescribed in chapter 10 of SECNAVINST 5510.36. To the extent possible, areas in which classified material are stored will be limited.
2. Report any weakness or deficiency in equipment being used to safeguard classified material in storage to the Command Security Manager (B 054). Reports must fully describe the weakness or deficiency and how it was discovered.
3. Valuables such as money, jewels, precious metals, narcotics, etc., will not be stored in the same containers used to safeguard classified material.
4. There shall be no external markings revealing the classification level of information being stored in a specific security container, vault, or secure room. Priorities for emergency evacuation and destruction shall not be marked or posted on the security container. This does not preclude the placing of required decals and necessary information for other purposes.

17001. STORAGE REQUIREMENTS

1. Chapter 10 of SECNAVINST 5510.36 must be reviewed prior to storing classified material.
2. Each security container will have a Security Container Records Form, Optional Form 89 (figure 17-1). Security containers will be inspected periodically. Records of inspection will be kept in the container.
3. Only approved filing cabinets will be used for storage of classified materials.

4. Field safes, one-drawer and two drawers lightweight General Services Administration approved security containers are used primarily for storage of classified material in the field and in transportable assemblages. Such containers must be rendered non-portable (i.e., chained to a permanent fixture), or guarded to prevent theft.

5. Authorization to store classified material in any office space will be requested from the Command Security Manager (B 054). A Physical Security Evaluation (PSE) will be conducted to determine the degree of security afforded by the existing area, and to recommend additional security requirements when necessary. No classified storage is authorized without this evaluation. Additional security containers will not be procured until:

a. A PSE of existing equipment and a review of classified records on hand has been made.

b. It has been determined that it would not be feasible to use available equipment or to retire, return, declassify, or destroy a sufficient volume of records currently on hand to make the needed security storage space available.

6. "Locked/Open" signs (Optional Form 95) will be displayed on each container that contains classified material to indicate whether the container is locked or open.

7. The following statement will be attached to the front of all security containers that are not being used for storage of classified material: "THIS CONTAINER NOT USED FOR STORAGE OF CLASSIFIED MATERIAL".

17002. COMBINATIONS, LOCKS, AND KEYS

1. Guidance pertaining to combinations, locks, and keys is contained in chapter 10 of SECNAVINST 5510.36.

2. Combination changes, neutralization of lockouts and repairs, or maintenance of security containers will be requested through the Base Locksmith by submission of a Work Request (Maintenance Management), NAVFAC Form 9-11014/20. Only trained personnel with the appropriate security clearance will make combination changes. Depending on the availability of trained security personnel the Command Security Manager (B 054) can provide assistance for changing combinations upon request.

3. Records of combinations will be sealed in a Security Container Information Envelope, SF 700 (figure 13-1), and kept on file at the Classified Material Control Center (CMCC) by the Command Security Manager, multiple envelopes will be maintained at SCP in a designated master container. Combination envelopes to master containers and vault/safe rooms lending access to master containers will be turned in to the CMCC for safekeeping. The Secondary Control Point (SCP) Custodian will inspect the SF 700 envelopes maintained in the master container monthly for signs of tampering. Part one of the SF 700 will be attached inside of the container, visible to those who might find the container left open. All security containers will be identified in Block 5 on the SF Form 700 by serial number. Do not identify any security container simply as, for example, "Safe #1."

4. When securing security containers, (vaults/strong rooms, safes, files, or cabinets) rotate dial or combination lock at least four complete turns in the same direction when securing.

5. When a container with a built in lock or a padlock is taken out of service, the built-in lock will be reset to the standard combination 50-25-50, and combination padlocks will be reset to the standard combination 10-20-30.

17003. PROCUREMENT AND TURN-IN OF SECURITY CONTAINERS

1. New security containers will not be requested or requisitioned by activity heads if similar equipment is available from the Assistant Chief of Staff, G-5.

2. When GSA approved security containers are no longer required or are not being used for storage of classified material, the using activity will turn in the container to the Assistant Chief of Staff, G-5.

3. The Command Security Manager will maintain listings of all security containers used for the storage of classified material. The Command Security Manager will be kept informed of all movements, change of possessions, and/or turn-ins of all approved security containers between and among divisions/activities/commands.

17004. DESTRUCTION OF CLASSIFIED INFORMATION

1. Prior to the destruction of classified information, review paragraph 10-17 of SECNAVINST 5510.36.

2. Destroy classified information no longer required for operational purposes per SECNAVINST 5212.5D. Destruction of classified information shall be accomplished by means that eliminate risk of recognition or reconstruction of the information.

3. Commanding officers will establish at least 1 day each year as "clean-out" day, when specific attention and effort are focused on disposition of unneeded classified and unclassified information.

4. Refer to CMS-1A and CMS-21A for the destruction of COMSEC information. Refer to DoD 5105.21-M-1 for destroying SCI, and OPNAVINST C5510.101D for destroying NATO information. For the destruction of all AIS media use NAVSO P-5239-26.

5. The Directorate for Information Systems Security, National Security Agency, provides technical guidance concerning appropriate methods, equipment and standards for the destruction of classified electronic media and processing equipment components, e.g., floppy disks, zip disks, jazz drive disks, CD ROM disks, hard drives, and magnetic tapes (audio, video and data). Once this medium type is associated with a classified source it is forever classified and the CMCC is the only authorized activity to implement the destruction of such information.

17005. DESTRUCTION METHODS AND STANDARDS

1. Various methods and equipment may be used to destroy classified information that include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition, or pulverizing.

2. A crosscut shredder shall reduce the information to shreds no greater than 3/64 inch wide by 1/2 inch long. Strip shredders will no longer be used for the destruction of classified information. Strip shredders and other shredders in use that do not meet the minimum standards for the destruction of classified material will have the following statement visibly attached, "THIS SHREDDER IS NOT AUTHORIZED FOR THE DESTRUCTION OF CLASSIFIED INFORMATION".

3. Pulverize machines and disintegrators must have a 3/32 inch or smaller security screen.

4. Pulping (wet process) devices with a 1/4 inch or smaller security screen may be used to destroy classified water-soluble material.

5. The CMCC has an industrial shredder for the destruction of large amounts of classified information. However, the following restrictions apply:

a. Only secret and confidential information may be destroyed. The shredding of unclassified information described in paragraph 17007 will not be authorized.

b. Items must be free of all metal, (i.e., paperclips and all fasteners); no cardboard or hard back folders. No soft or hard plastic items of any kind will be placed in the shredder for destruction.

c. To ensure that the equipment is operated properly, a representative from the CMCC must be present at all times. SCPs are to provide their own transportation for material and personnel to conduct the destruction.

d. Destruction times will be scheduled by appointment only.

17006. DESTRUCTION PROCEDURES

1. Strict adherence to the procedures for the destruction of classified material and the methods of the destruction contained in chapter 10 of SECNAVINST 5510.36 and this manual will be observed.

2. A record of destruction is required for Top Secret information. The use of OPNAV 5511/12, "Classified Material Destruction Report," is no longer required. See paragraph 10-19 of SECNAVINST 5510.36 for current methods of destruction.

3. Per SECNAVINST 5510.36, a record of destruction is not required for Secret and Confidential information; however, at MCB, Quantico, a requirement for reporting the destruction of Secret information will be in effect. All information being controlled under the Automated Security Control Program (ASCP) will be destroyed as follows:

a. When controlled secret document(s) are destroyed at the SCP level, a destruction report will be generated via the ASCP, and forwarded to the Document Control Section (DCS) at the CMCC. The destruction report must be signed and witnessed by the appropriately cleared personnel as the information is placed into the burn bag or actually destroyed. Retain a signed copy of the report until those document(s) destroyed no longer appear in the SCP database, or for 2 years.

b. When controlled secret documents are to be destroyed by the DCS at the CMCC, print a destruction report via the ASCP and forward to the DCS, along with the document(s)/material to be destroyed. The SCP retains a signed copy of the report until those document(s) destroyed no longer appear in the SCP database, or for a period of 2 years.

4. When secret message traffic, working papers, and all other classified documents not controlled by the ASCP are destroyed, use OPNAV 5511/12 and retain locally for 2 years. Confidential material and classified waste do not need a record of destruction. However, it is highly recommended that a record of destruction be made and retained by the custodian for protection of that individual and this Base.

5. North Atlantic Treaty Organization (NATO) secret and confidential destruction reports must be recorded on a separate OPNAV Form 5511/12 and forwarded to the Command Security Manager (NATO Control Point Officer) for forwarding to the CMC Sub registry. Records of destruction will be retained for 2 years.

17007. DESTRUCTION OF UNCLASSIFIED MATERIAL

1. Destroy record copies of FOUO, SBU, DoD UCNI, DOE UCNI, Sensitive (Computer Security Act of 1987), and unclassified technical documents assigned distribution statements B through X, per SECNAVINST 5212.5D, Navy and Marine Corps Records Disposition Manual, 22 Apr 98. Non-record copies may be shredded or torn into pieces and placed in trash containers. Records of destruction are not required.

2. Destroy Unclassified Drug Enforcement Administration Sensitive Information and Naval Nuclear Propulsion Information (NNPI) in the same manner approved for classified information.

3. Unclassified material, including formally classified material that has been declassified, For Official Use Only (FOUO) material, and unclassified messages do not require the assurance of complete destruction.

4. Contrary to widespread opinion, there is no security policy requiring destruction of unclassified messages (except NNPI). Tearing messages into pieces (as is done with FOUO material), defacing them before discarding, or using classified destruction methods are among the choices left to commanding officers and activity heads.

INFORMATION AND PERSONNEL SECURITY PROGRAM

NOTE: Store this form in the security container or on the vault door.

TYPE <input type="checkbox"/> SECURITY CONTAINER <input type="checkbox"/> VAULT DOOR		SERIAL NUMBER (Container: Located on the side of the container drawer. Vault Door and Map and Plan Container: Located on the inside face of the door.)			
MANUFACTURER		GSA CLASS <input type="checkbox"/> ONE <input type="checkbox"/> TWO <input type="checkbox"/> THREE <input type="checkbox"/> FOUR <input type="checkbox"/> FIVE <input type="checkbox"/> SIX <input type="checkbox"/> SEVEN			
OPERATING PROBLEM	TYPE OF MAINTENANCE	DATE REPAIRED/ INSPECTED	TECHNICIAN		ORGANIZATION NAME
			NAME	ACTIVITY	
SIGNATURE OF RESPONSIBLE OFFICIAL		NAME OF RESPONSIBLE OFFICIAL			DATE SIGNED

FRONT

OPERATING PROBLEM	TYPE OF MAINTENANCE	DATE REPAIRED/ INSPECTED	NAME	ACTIVITY	NAME
SIGNATURE OF RESPONSIBLE OFFICIAL		NAME OF RESPONSIBLE OFFICIAL			DATE SIGNED

BACK

Figure 17-1.--Sample Security Container Records Form (Optional Form 89).

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 18

INDUSTRIAL SECURITY PROGRAM

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	18000	18-3
AUTHORITY	18001	18-3
INDUSTRIAL SECURITY MISSION	18002	18-4
CLEARANCE UNDER THE NISP	18003	18-4
DSS AND COMMAND SECURITY OVERSIGHT OF CLEARED DOD CONTRACTOR OPERATIONS.	18004	18-5
FACILITY ACCESS DETERMINATION (FAD) PROGRAM	18005	18-6
CONTRACT SECURITY CLASSIFICATION SPECIFICATION (DD 254)	18006	18-6
CONTRACTING OFFICER'S REPRESENTATIVE (COR) INDUSTRIAL SECURITY RESPONSIBILITIES .	18007	18-6
TRANSMISSION OR TRANSPORTATION	18008	18-7
FIGURE		
18-1 SAMPLE CONTRACT SECURITY CLASSIFICATION SPECIFICATION (DD 254)		18-9

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 18

INDUSTRIAL SECURITY PROGRAM

18000. BASIC POLICY

1. Chapter 11 of SECNAVINST 5510.36 will be utilized as a source reference document for the Industrial Security Program.
2. Commanding officers shall establish an Industrial Security Program if their commands engage in classified procurement or when cleared DoD contractors operate within areas under their direct control. Command security procedures shall include appropriate guidance, consistent with this regulation, to ensure that classified information released to industries is safeguarded.
3. Commanding officers responsible for the acquisition of classified defense systems shall comply with the requirements of DoD 5200.1-M, which establishes policy and assigns responsibilities for identifying and protecting classified information or controlled unclassified information that has been identified as critical to the combat effectiveness of systems being developed within the DON acquisition programs.
4. Commanding officers responsible for the acquisition of classified defense systems shall develop a Program Protection Plan (PPP) to fulfill the requirements of DoD 5200.1-M. Because contractor facilities are included, cleared DoD contractors may assist in developing the PPP for a classified contract. Requirements levied on contractors in the PPP shall be conveyed in the contract document itself or on the Contract Security Classification Specification Form, DD Form 254 (see figure 18-1).

18001. AUTHORITY

1. Executive Order 12829, National Industrial Security Program (NISP), 6 Jan 93, established the NISP for safeguarding information released to industry classified under Executive Order 12958, Classified National Security, or its successor or predecessor orders, and SECNAVINST 5510.30A. This regulation implements the requirements of the NISP within the DON. Provisions of this regulation relevant to operations of cleared DoD contractor employees entrusted with classified information shall be applied by contract or other legally binding instrument.

2. DoD 5200.1-M imposes the requirements, restrictions, and safeguards necessary to prevent unauthorized disclosure of classified information released by U.S. Government Executive Branch departments and agencies to their contractors.

3. DoD 5220.22-M, Supp 1 imposes requirements, restrictions, and safeguards necessary to protect special classes of information beyond those established in the baseline portion of reference DoD 5220.22-M.

18002. INDUSTRIAL SECURITY MISSION

1. The chief operating officer for Defense Security Service (DSS) oversees DoD implementation of the NISP through 12 Operations locations (OPLOCs) throughout the CONUS. An additional OPLOC will be established to oversee the international aspects of the NISP (formerly known as Office of Industrial Security International). OPLOCs provide administrative assistance and policy guidance to local DSS field elements charged with security oversight of cleared DoD contractors located in CONUS that perform on classified contracts. Consult the DSS Homepage at <http://www.dss.mil> for information pertaining to various DSS functions.

2. DSS, Operations Center Columbus (OCC) grants personnel clearances to individuals in private industry who require access to classified information in order to perform their jobs. The OCC also grants Facility (Security) Clearances (FCL) within the NISP, refers cases with major adverse information to the Defense Office of Hearings and Appeals for adjudication, processes overseas visit requests, and responds to requests for information regarding personnel clearances and FCL applications, and facility storage capability.

18003. CLEARANCE UNDER THE NISP. An employee of a contractor granted an FCL under the NISP may be processed for a personnel clearance when the contractor determines that access is essential in the performance of tasks or services related to a classified contract or an IR&D Program (see chapter 8, paragraph 8-8 of SECNAVINST 5510.30A) for contractor granted clearances, Interim Secret and Confidential personnel clearances, Limited Access Authorizations (LAA), and adverse information reporting).

18004. DSS AND COMMAND SECURITY OVERSIGHT OF CLEARED DoD CONTRACTOR OPERATIONS

1. Shipboard. Onboard ship cleared DoD contractor employees have visitor status and shall conform to the requirements of this and command security regulations. Cleared DoD contractors shall submit written requests to the commanding officer who will then grant approval for classified visits by employees to the ship.

2. Shore Installations. Commanding officers shall establish or coordinate security oversight over classified work carried out by cleared DoD contractor employees in spaces controlled or occupied at DON shore installations. Command oversight shall be carried out by exercising one of the following options:

a. The commanding officer requests, in writing, that the DSS OCC grant the contractor an FCL and that DSS assume security oversight.

b. The commanding officer requests, in writing, that the DSS OCC grant the contractor an FCL with the command retaining security oversight. Commands shall conduct periodic reviews and forward a copy of the Industrial Security Inspection Report to the DSS OPLOC which exercises geographic jurisdiction over the installation. Contractors granted an FCL under these first two options assume the status of a tenant activity.

c. The commanding officer determines that the contractor is a short or long-term visitor and decides that an FCL is not warranted. Contractor employees shall conform with command security regulations and shall be included in the command Security Education Program.

3. Off-site Locations. When contractors perform work at locations other than the command awarding the contract, the awarding command shall inform the new host. Forward to the host command a copy of the notification of contract award, a copy of the DD 254, and other pertinent documents.

4. DON Overseas Locations. Local commands that award classified contracts requiring performance by cleared DoD contractors at DON overseas locations shall ensure that SECNAVINST 5510.36 is enforced in all aspects of contract security administration.

18005. FACILITY ACCESS DETERMINATION (FAD) PROGRAM

The Internal Security Act of 1950 entrusts commanding officers to protect persons and property against the actions of untrustworthy persons. SECNAVINST 5510.36 confirms the FAD Program within the DON to assist commands in making trustworthiness determinations on contractor employees for access eligibility to controlled unclassified information or sensitive areas and equipment under DON control. Trustworthiness determinations pertain to unclassified contracts for various services (e.g., janitorial, guards, equipment maintenance). Commands shall take the necessary steps to include the conditions of the FAD Program in the specifications of all contracts needing trustworthiness determinations, thereby eliminating the necessity to award a classified contract for performing services only. SECNAVINST 5510.30A addresses specific requirements for administering the FAD Program.

18006. CONTRACT SECURITY CLASSIFICATION SPECIFICATION (DD 254)

Commanding officers shall ensure that a DD 254 is incorporated into each classified contract. The DD 254, with its attachments, supplements, and incorporated references, is designed to provide a contractor with the security requirements and classification guidance needed for performance on a classified contract. An original DD 254 shall be issued with each request for proposal, other solicitations, contract award, or follow-on contract to ensure that the prospective contractor is aware of the security requirements and can plan accordingly. A revised DD 254 shall be issued as necessary during the lifetime of the contract when security requirements change. A final DD 254 shall be issued on final delivery or on termination of a classified contract. (See figure 18-1 for a sample DD 254.)

18007. CONTRACTING OFFICER'S REPRESENTATIVE (COR) INDUSTRIAL SECURITY RESPONSIBILITIES

1. Paragraph 2001 identifies the appointment of a qualified security specialist as a COR.

2. The following industrial security responsibilities are normally assigned to the COR, but are not limited to the following:

a. Review statement of work to ensure that access to or receipt and generation of classified information is required for contract performance.

b. Validate security classification guidance, complete, and sign the DD 254:

(1) Coordinate review of the DD 254 and classification guidance.

(2) Issue a revised DD 254 and other guidance as necessary.

(3) Resolve problems related to classified information provided to the contractor.

c. Provide, when necessary, in coordination with the program manager, additional security requirements beyond those required by this regulation in the DD 254 or the contract document itself.

d. Initiate all requests for FCL action with the DSS OCC.

e. Verify the FCL and storage capability prior to release of classified information.

f. Validate justification for Interim Top Secret Personnel Clearance Levels and FCLs.

g. Validate and endorse requests submitted by industries for LAAs for non-U.S. citizen employees of cleared contractors.

h. Coordinate, in conjunction with the appropriate transportation element, a suitable method of classified shipment when required.

i. Review requests by cleared contractors for retention of classified information beyond a 2-year period and advise the contractor of disposition instructions or issue a final DD 254.

j. Certify and approve Registration For Scientific and Technical Information Services requests (DD 1540).

k. Review reports of security violations and compromises within industries and forward to program managers.

l. Ensure that timely notice of contract award is given to host commands when contractor performance is required at other locations.

18008. TRANSMISSION OR TRANSPORTATION

1. Appropriately cleared and designated DoD contractor employees may act as couriers, escorts, or handcarriers provided that:

a. They have been briefed by their facility security officer on their responsibility to account for and safeguard classified information;

b. They possess an identification card or badge which contains their name, photograph, and the company name;

c. Employees retain classified information in their personal possession at all times. Arrangements shall be made in advance of departure for overnight storage at a U.S. Government installation or at a cleared contractor's facility that has appropriate storage capability; and,

d. The transmission or transportation meets all other requirements specified in chapter 16 of this manual.

2. Appropriately cleared DoD contractors may use the General Services Administration commercial contract carrier for overnight delivery of Secret and Confidential information to U.S. Government agencies within CONUS when procedures have been formally approved by the Defense Security Service OPLOC prior to starting such transmissions (see ISL 97-1, Industrial Security Letter, Jul 97).

3. To address the following subjects, refer to chapter 11 of SECNAVINST 5510.36.

- a. Contractor Badges.
- b. Contractor Facility Clearances.
- c. Disclosure.
- d. Release of Intelligence to Cleared DoD Contractors.
- e. Prohibited Release of Intelligence.
- f. Sanitization of Intelligence.

INFORMATION AND PERSONNEL SECURITY PROGRAM

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING	
				a. FACILITY CLEARANCE REQUIRED	
				b. LEVEL OF SAFEGUARDING REQUIRED	
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>			3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>		
a. PRIME CONTRACT NUMBER			a. ORIGINAL <i>(Complete date in all cases)</i>		Date (YYMMDD)
b. SUBCONTRACT NUMBER			b. REVISED <i>(Supersedes all previous specs)</i>		Revision No. Date (YYMMDD)
c. SOLICITATION OR OTHER NUMBER		Due Date (YYMMDD)	c. FINAL <i>(Complete Item 5 in all cases)</i>		Date (YYMMDD)
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.					
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input type="checkbox"/> NO. If Yes, complete the following: In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____					
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>					
a. NAME, ADDRESS, AND ZIP CODE			b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE			b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>
8. ACTUAL PERFORMANCE					
a. LOCATION			b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT					
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION				a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	
b. RESTRICTED DATA				b. RECEIVE CLASSIFIED DOCUMENTS ONLY	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION				c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	
d. FORMERLY RESTRICTED DATA				d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	
e. INTELLIGENCE INFORMATION:				e. PERFORM SERVICES ONLY	
(1) Sensitive Compartmented Information (SCI)				f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	
(2) Non-SCI				g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	
f. SPECIAL ACCESS INFORMATION				h. REQUIRE A COMSEC ACCOUNT	
g. NATO INFORMATION				i. HAVE TEMPEST REQUIREMENTS	
h. FOREIGN GOVERNMENT INFORMATION				j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	
i. LIMITED DISSEMINATION INFORMATION				k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	
j. FOR OFFICIAL USE ONLY INFORMATION				l. OTHER <i>(Specify)</i>	
k. OTHER <i>(Specify)</i>					

DD Form 254, DEC 90

Previous editions are obsolete.

S/N 0102-LF-011-5800 805/340

Figure 18-1.--Sample Contract Security Classification Specification (DD 254).

INFORMATION AND PERSONNEL SECURITY PROGRAM

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release. <div style="display: flex; justify-content: space-between; align-items: center;"><div><input type="checkbox"/> Direct</div><div><input type="checkbox"/> Through (Specify):</div></div>		
<div style="font-size: small; margin-top: 10px;">to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review. * In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.</div>		
13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)		
14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.) <div style="text-align: right;"><input type="checkbox"/> Yes <input type="checkbox"/> No</div>		
15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.) <div style="text-align: right;"><input type="checkbox"/> Yes <input type="checkbox"/> No</div>		
16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.		
a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (Include Area Code)
d. ADDRESS (Include Zip Code)		17. REQUIRED DISTRIBUTION <div style="margin-top: 5px;"><input type="checkbox"/> a. CONTRACTOR</div> <div style="margin-top: 5px;"><input type="checkbox"/> b. SUBCONTRACTOR</div> <div style="margin-top: 5px;"><input type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR</div> <div style="margin-top: 5px;"><input type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION</div> <div style="margin-top: 5px;"><input type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER</div> <div style="margin-top: 5px;"><input type="checkbox"/> f. OTHERS AS NECESSARY</div>
e. SIGNATURE		

DD Form 254 Reverse, DEC 90

U.S. GOVERNMENT PRINTING OFFICE: 1994-504-079/00376

Figure 18-1.--Sample Contract Security Classification Specification (DD 254) (Continued).

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 19

LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY	19000	19-3
* DISCOVERY OR SUBJECTION TO COMPROMISE. . .	19001	19-3
* OTHER SECURITY VIOLATIONS.	19002	19-4
* UNSECURED CONTAINERS	19003	19-4
* IMPROPER TRANSMISSION	19004	19-5
* INFORMATION SYSTEMS.	19005	19-5

INFORMATION AND PERSONNEL SECURITY PROGRAM

CHAPTER 19

LOSS, COMPROMISE, AND OTHER SECURITY VIOLATIONS

* 19000. BASIC POLICY. There are two types of security violations. One results in a compromise or a possible compromise of classified information. The other is when security regulations are violated but no compromise occurs. Compromise is the disclosure of classified information to a person who is not authorized access. Security violations of either type must be reported to the Comdr MCB (B 054), where a vigorous investigation will be initiated and the problems causing the violation corrected rather than covered up. Amplifying instructions are contained in chapter 12 of SECNAVINST 5510.36.

* 19001. DISCOVERY OR SUBJECTION TO COMPROMISE

1. Any individual who becomes aware of a compromise or subjection to compromise of classified information will immediately notify the activity security manager, activity head, and the custodian. Once notified, all pertinent information will be reported to the Comdr MCB (B 054) as soon as possible by telephone. A brief, typed report of the violation will be made by the responsible activity head to the Comdr MCB (B 054) via the operational chain of command by 1600 the following workday. This report will briefly address the circumstances causing the incident, pinpoint responsibility, and attempt to determine the degree of compromise. In the event an open security container is found, a 100 percent inventory of the container contents will be made, and a copy of said inventory forwarded to the Comdr MCB (B 054) and to the Head, Classified Material Control Center (CMCC).

2. Upon receipt of a report, the Comdr MCB (B 054) will direct a preliminary inquiry per paragraph 12-2.2 of SECNAVINST 5510.36. Normally, this inquiry will be conducted by the activity having custodial responsibility of the material. However, as circumstance dictate, an inquiry may be conducted by a person not attached to the reporting activity. When investigative support is required or circumstances warrant the use of trained investigators, the Comdr MCB (B 054) may request that Naval Criminal Investigative Service personnel assist in or conduct the preliminary inquiry. When a preliminary inquiry is directed, the inquiry will be completed

INFORMATION AND PERSONNEL SECURITY PROGRAM

quickly, usually within 72 hours. The Comdr MCB (B 054) will, upon receipt, comply with the guidance set forth in chapter 12 of SECNAVINST 5510.36.

3. Upon completion of the preliminary inquiry, the Comdr MCB (B 054) will determine if a command investigation is warranted. The A/CS G-1 MCB will select proposed investigating officers and forward the determination the C/S MCB, who will issue the convening order. The convening order must recite the specific purpose of the inquiry. The appointed investigating officer will conduct his investigation per chapter 12 of SECNAVINST 5510.36. The reference is available in the office of the Command Security Manager, MCB.

4. The overriding priority, upon receiving a report of compromise or subsection to compromise is to regain custody of the classified information, and or contain spillages where possible.

- * 19002. OTHER SECURITY VIOLATIONS. Security violations occurring during or after normal duty hours will be immediately reported to the activity security manager and activity head. A followup report will be made as soon as possible to the Comdr MCB (B 054) via telephone. A complete typed report of the violation will be made by the activity head to the Comdr MCB (B 054) via the chain of command by 1600 the following day. This action will require hand carrying of the report ("walk through" procedures).
- * 19003. UNSECURED CONTAINERS. If a container in which classified material is stored is found unlocked in the absence of assigned personnel, report the incident immediately to the duty officer. The location will be guarded until the duty officer arrives at the location of the unlocked container. The duty officer will then inspect the classified material, lock the container, and make contact with the person responsible for the container, requiring them to return to make a complete inventory. A copy of the inventory will be forwarded to the Comdr MCB (B 054) and to the Head, CMCC (B 054).

INFORMATION AND PERSONNEL SECURITY PROGRAM

- * 19004. IMPROPER TRANSMISSION. When an activity aboard this Base receives classified material which shows improper handling, notify the Comdr MCB (B 054) so that immediate notification to the CO of the sending activity can be made.

- * 19005. INFORMATION SYSTEMS. In addition to the above, any security violations involving a computer, computer system, network (SIPRNET/NIPRNET), or other electronic media must be immediately reported to the Information Systems Security Manager, G-6, MCB, Quantico. Examples of such violations are improperly marked classified disk, CDs, spillage, receipt of improperly transmitted materials, etc.. Immediate reporting cannot be over emphasized due to the nature of the violation and how quickly some violations can spread if not immediately contained.